PERFORMANCE WORK STATEMENT

For

Federal Service Desk (FSD)
Contact Center

A procurement by the
U.S. General Services Administration
on behalf of
Office of Systems Management (QD)
Integrated Award Environment (IAE)
Washington, D.C.

Solicitation Number: ID15190008
Contract Number TBD

This requirement is being solicited as a Task Order under the
GSA Alliant 2 Government-wide Acquisition Contract

NAICS: 541519 - Other Computer Related Services
Product Service Code: D321 - IT & Telecommunications Help Desk

Table of Contents

1. BACKGROUND

1.1 Government Mission & Procurement Objective

The mission of the GSA Office of Integrated Award Environment (IAE) is to support a common, secure business environment that facilitates and supports cost-effective acquisition of, and payment for, goods and services; effective management of federal acquisition and assistance awards; and consistent transparency into federal acquisition and assistance awards.

The largest and most complex of the e-Government (e-Gov) initiatives, the IAE works on behalf of the acquisition and financial assistance communities to save money, be more efficient, reduce burdens on the communities we serve, deliver value to users, and improve federal award management.

1.2 Procurement Objective

The purpose of this procurement is to obtain the necessary contractor support to answer user questions and facilitate a successful customer experience when using IAE systems. To meet this objective, the contractor shall operate the Federal Service Desk (FSD) Contact Center, which serves as the primary point of contact for IAE system users to engage with the government or receive assistance from the government, to perform tasks in IAE systems. System users rely on the FSD for accurate, complete and timely information delivered in a professional and courteous manner. As such, the government has a need for a contact center with state-of-the-art technical tools, that promotes strong user engagement, and comprehensive knowledge management capabilities to serve a broad range of customers. The overarching government requirement is for contact center services and related state-of-the-art technical tools so that the customer experience is one that enables customers to easily perform the work or seek the information for both the private and public sectors.

The IAE Program works, namely, using Scaled Agile Framework (SAFe) methodology and best practices, so the awarded offeror will be required to collaborate across all boundaries of the development and enhancement of (beta).SAM.gov. The success to-date of the IAE Program is contingent on the use of SAFe. By not working in a traditional, waterfall-siloed manner but flexibly and incrementally the program delivers value to IAE users, both in how (beta).SAM.gov operates and by accurately resolving service desk issues from users rapidly.

The modernized SAM currently has a Joint Product Team (JPT) plus 16 teams that capture the DevOps (development and operations) Portfolio Epics, Epics, and User Stories work currently in Atlassian's JIRA and Confluence tools; that work is hosted on the FAS Cloud Services (FSC) platform (formerly named the Business Services Platform or BSP). The teams use the Atlassian Agile Lifecycle Management tool, JIRA

(currently version 7.12.3), to track SAFe progress of the work in incremental releases, which also acts as a ticketing system; within JIRA there is an internal ticketing process call JAT to make changes to the tool. The teams also interact with the GSA IT instance of ServiceNow enterprise to resolve platform-related technical issues.

It is anticipated that the FSD.gov website will eventually be retired and the functionality found there will be accessed from (beta.)SAM.gov. (beta.)SAM.gov is not a "beta" site, but is an actual online production site. This site is currently named beta.SAM.gov until it is migrated from legacy SAM.gov to beta.SAM.gov. In the future, the site will be named solely SAM.gov. Customers will come to (beta.)SAM.gov to:

- Create and maintain their accounts including Multi Factor Authentication (MFA) as per NIST 800-63 standard for AAL Level 2.
  - GSA currently uses login.gov
- Utilize user profile information to pre-populate a ticket
- Create chats
- Complete web-form requests
- Access knowledge-based materials
- View FSD Service Level Agreement (SLA)-based data and status information (wait times)
- View individual ticket status/responses to FSD
- View FSD messages and announcements including alerts and outages

1.3 IAE Program History

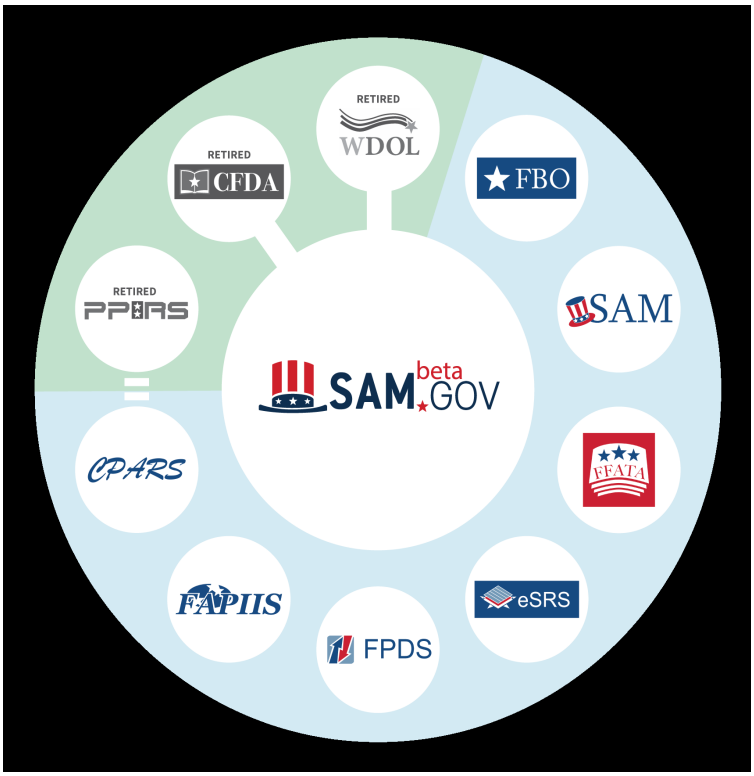
The current IAE systems were developed over several years as free-standing, web-based systems to fulfill different roles throughout the acquisition and grants-making process. They are operated and maintained by multiple independent contractors.

Current IAE systems consist of the following:
- Contractor Performance Assessment Reporting System (CPARS)
- Electronic Subcontracting Reporting System (eSRS)
- Federal Awardee Performance and Integrity Information System (FAPIIS)
- Federal Business Opportunities (FedBizOpps)
- Federal Funding Accountability and Transparency Act Subaward Reporting System (FSRS):
- Federal Procurement Data System (FPDS:
- System for Award Management (SAM)
- beta.SAM.gov

IAE has already completed the migration of CFDA and WDOL to beta.SAM.gov and merged PPIRS into the CPARS past performance system, and intends to merge the eight remaining systems into beta.SAM.gov as shown in the representation below. After the migration of SAM.gov in beta.SAM.gov, the site will be known as SAM.gov. This is a multi-year effort to create a more modern and unified user experience that provides:

- single web application that requires a single user account and a single, more accurate search across all of our award data sets;
- single, role-driven workspace to track award data;
- data services providing award data in multiple formats, including Application

Programing Interface (API) and file extracts;
- data bank services with formatted and adhoc reports;
- reference services with consistent data reporting (state, zip code, congressional district, North American Industrial Classifications, etc.);
- searchable learning center with videos, glossary, FAQs, articles, alerts, and release notes; and
- seamless access to customer service.



IAE is governed by the Award Committee for eGov (ACE) structure which includes the Procurement Committee for eGov (PCE) and the Financial Assistance Committee for eGov (FACE). Additionally, all IAE operations are coordinated and prioritized through a Change Control Board (CCB) that consists of voting representatives from each of the 24 Chief Financial Officer (CFO) Act agencies. These same agencies contribute funding for the IAE operations. IAE is also governed through the GSA Senior Management Leadership and is co-led by the Federal Acquisition Service (FAS) and GSA IT Office of the Chief Information Officer (CIO).

Federal Service Desk (FSD) is the current contact center for all users seeking assistance with the IAE systems (except for FAPIIS and CPARS which are handled under a separate contract). FSD receives calls, chats and web-forms from both domestic and international members of the federal acquisition and assistance community as well as the public. FSD is a contact support center only and does not provide any physical IT support, equipment support or user software upgrades.

The current call center, FSD, has a contact (calls, chats, web-forms, etc.) volume of over 36,000 contacts a month. In fiscal year (FY) 2019, the estimated annual contact volume was approximately 430,000 with significantly increased volume planned within the scope of this future contract award. Please see Attachment A - FSD Contact Center Data. FSD live agent assistance is available from 8:00 a.m. EST to 8:00 p.m. EST five days a week (excluding Federal holidays). The site is available 24 hours for user assistance via self-help assistance. Currently, the FSD.gov site is managed as an independent site operated separately from the IAE applications, supporting both legacy IAE systems and the new beta.SAM.gov (eventually SAM.gov) modernization platform.

1.4 IAE Current Status

The federal government, according to USASpending.gov, awarded over $4.11 trillion dollars in contracts, grants, loans, and other federal assistance to entities in FY 2018. Entities awarded federal procurement and financial assistance actions, with limited exceptions, are required to use IAE systems to register, report, and discover opportunities for participation in the federal award process. IAE systems are used extensively by government personnel during all aspects of the procurement and financial assistance processes and are based on federal statute and policy. Of the reported federal contracts that were awarded, IAE systems currently track approximately $1.1 trillion and 60 million transactions annually. With growing numbers, IAE currently has over one million registered users and over 500 million hits or page views, per month.

2. ORIENTATION

2.1 General Scope of Work

This Performance Work Statement (PWS) defines program support objectives for Federal Service Desk (FSD) Contact Center and eventually the SAM.gov learning center.

Work will be performed over a period of five years, with an anticipated Base Period of 12 months and four Option Periods of 12 months each.

2.2 Resources

Under this contract/task order, unless otherwise stipulated (see Section 13 – Government Furnished Items), the Contractor shall furnish or provide all personnel, personnel management and supervision, all related internal supporting business functions including background and overhead personnel, materials, supplies, equipment, and facilities to perform the full range of technical and administrative services required by this contract.

During the course of this contract/task order, the Government may make additional Government Furnished Items (GFIs) -- materials, equipment, and facilities -- available upon receipt of a written request from the Contractor to the Government Technical Representative. These GFIs, if provided, would be in addition to those initially set forth in Section 13 - Government Furnished Items.

The contractor shall provide fully trained personnel. (Reference "Staff Employee Requirement" in Section 7.)

Government personnel will be made available to confirm technical and security standards, coordinate integration with IAE systems, answer questions, review and approve completed draft deliverables, provide feedback, and provide shipping directions for deliverables.

2.3 Placement and Management of Work

All work under this Contract/Task Order will be performed as described, and within the scope of this PWS. Clarification to the work may be provided to the Contractor in writing by the Contracting Officer's Representative (COR) using a Technical Directive form or other agreed upon written documentation. Contractor employees shall perform work as specified in this Contract/Task Order as directed by the Contractor's designated project manager, who shall have full responsibility for the assignment and monitoring of Contractor employee activities. All work shall be performed within the scope of this PWS and the Government will not ask or require the Contractor to perform work that is outside of the scope of this Contract/Task Order.

2.4 Customers

The customer and recipient of all work performed under this contract order is:
Office of Systems Management, IAE
Office of Stakeholder Management (QD)
1800 F Street, NW, HUB G030
Washington, DC 20405

2.5 Performance Monitoring

Contractor performance shall be monitored by the Government representatives in accordance with the government-approved Contractor's Quality Control Plan (QCP) and the Government's Quality Assurance Surveillance Plan (QASP) (see Section 12, below).

2.6 General Definitions

CO: Government Contracting Officer

CONTACT: An end user request for assistance. This can be in response to an email, chat session, live telephone call, self-generated service request, voicemail or any other medium available to the end user.

COR: Contracting Officer's Representative (See Section 15, below)

FCS: FAS Cloud Services: The next generation IT platform for hosting multiple Government–wide acquisition applications. FSC sits on Amazon Web Services (AWS).

FTE: Full Time Equivalent: The number of labor hours equal to those that would be worked by one employee in a year. For this procurement action 1960 hours is

considered an FTE.

CPARS: Contractor Performance Assessment Reporting System: This is a system that generates reports that are created by the government evaluators to document contractor performance.

Entity: Refers to organizations or individuals applying for financial assistance, contract awards, loans, grants, or who need to register to do business with the federal government including but not limited to sole proprietors, corporations, partnerships, government agencies, non-profits, etc.

EVS: Entity Validation Services: A method to determine uniqueness, which could include the assignment or use of a unique entity identifier (UEI) validation of certain data, and associated services.

IAE: GSA Office of Integrated Award Environment

IAE PMO: GSA Integrated Award Environment Project Management Office

NIST: National Institute of Standards and Technologies

Normal Workweek: A workweek is 40 hours.

Overtime: Time worked by a contractor's employee in excess of the employee's normal workweek. (Note: Premium pay is not authorized under this task order for overtime work.)

Quality Assurance: A planned and systematic pattern of all actions necessary to provide confidence to the government that adequate technical requirements are established; products and services conform to established technical requirements; and satisfactory performance is achieved. For the purpose of this document, Quality Assurance refers to actions by the government.

Quality Assurance Personnel (QAP): A functionally qualified government person(s) responsible for surveillance of contractor performance and providing communications to the contractor(s) and PCO.

Quality Assurance Surveillance Plan (QASP): A plan detailing the contract surveillance procedures and containing the Objectives, Measures and Expectations that will be used to evaluate contractor performance of the PWS objectives.

Quality Control: Those actions taken by a contractor to control the production of outputs to ensure that they conform to the contract requirements.

TO: Task Order

2.7 Technical Definitions

API: Application program interface

IAE Application Platform: The IT platform for hosting multiple Government–wide acquisition applications "on the cloud." See FCS.

PII: Personally Identifiable Information: Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

Real Time Response: Responses to interface requests that return a response within a few seconds of submission.

Warm Transfer (also known as a live or hot transfer): The call center operator who has received a call then dials a predetermined number. The operator \talks to the person who has picked up the call before transferring the caller. This could also be a three-way conference before the initial call center operator drops-off.

3. ASSUMPTIONS

The contractor shall employ a staff with sufficient experience and expertise to perform each of the tasks in PWS. IAE will be working in a Scaled Agile (Scaled Agile Framework or SAFe) manner and will be routinely enhancing and updating the functionality of IAE managed systems. Prior to release of code to production, the contractor will ensure that the contractor agents get trained on changes to the functionality of the systems and that scripts, documentation, training materials and escalation processes are updated to include the current functionality.

4. PRIMARY PERFORMANCE OBJECTIVES

4.1 Customer Experience Objective

The contractor shall meet this objective by providing technology necessary for day-to-day contact center operations including:

- Resolution of tickets (incidents, concerns, issues, requests, etc.).
- Telecommunication services (Transfer the existing 800 toll-free telephone number to the contractor) necessary to handle projected call volumes. Please see Attachment B –FSD Issue Type Hierarchal Volume
- Interactive Voice Response system (IVR)
- A web-based, Service Request Management system to effectively manage service requests received via (beta.)SAM.gov. The contractor shall provide access and train IAE Government and support contractor staff on the proposed Service Request Management System. This shall include initial system training, and user training for new users to be delivered by live webinars.
    - The contractor shall provide any required licenses, as Tools/ODCs, for the government's IAE Program Management Office (PMO), COR and other individuals that may include contractors as requested by COR, who

shall be granted access to the Service Request Management system, including read-only access to the raw data on IAE tickets. Currently there are approximately 260 licenses which are for both contractor and government use. The current license quantity may not reflect future program needs.

- A required FedRAMP authorized Service Request Management System (ticketing system) which shall be a cloud solution and FedRAMP authorized. as indicated at the below link:
  - https://marketplace.fedramp.gov/#/products?sort=productName
- A chat tool that is integrated within the ticketing system enabling the agent and customer to view the chat in the ticket.

As part of this objective, the government intends to leverage additional technology within the helpdesk framework to achieve reductions in abandoned call rate, resolution through self-help at lower tiers, improved user satisfaction and greater efficiency and cost reduction. This includes technologies such as blog technologies that allow users to self help or peer assist, and automated services could include, but are not limited to, Artificial Intelligence (AI), Chat Bots, Robotic Process Automation, Voice/Speech Recognition, Text-to-Speech, Voicemail Callback, Web Callback, Email, Hosted Email Web Form, API transmission of data from (beta.)SAM.gov to the contractor's system, etc.

All services provided, and products delivered outside IAE and (beta.)SAM.gov, must comply with government security and accessibility (Section 508 of the Rehabilitation Act of 1973) mandates. Third party service integrations with IAE or (beta).Sam.gov the interfaces should be included as part of the system boundary and should comply with GSA security and A&A requirements in accordance with our guides.

4.1.1 Creation of Training Support Materials

The government intends to provide training to our users on all functionality within IAE applications and intends to provide updates to that training for every transition or release of code into production. The Government will implement a user training strategy before, during, and after the release of the code into the production environment of the new platform. This effort supports IAE's goal to continue to reduce burden for both federal officials and recipients as well as a mechanism to reduce the number of overall contacts.

The contractor shall assist IAE with developing online training tools to address the training needs of federal agency customers, users, public users, and stakeholders for both the acquisition and assistance communities to include:

- Creating, editing and integrating required materials as directed by the government;
- Collaborating with the IAE and CIO team members on content, as well as other applicable offices;
- Revising, uploading, and storing training material in various mediums for user access in the (beta.)SAM.gov learning center; and materials as needed for current and future training needs;
- All created materials shall meet IAE design standards (Section 4.2.4)

- Provide Government with an up to date copy of all created materials.

The contractor shall create training material in various mediums to include written, graphical, audio, visual, etc. as needed by the government. Materials may take the form of:

- Frequently Asked Questions (FAQs)
- Webinars
- Announcements and change notices
- Pre-recorded demonstrative videos
- Articles on specific tasks or processes
- Glossaries
- Release notes for posting on (beta.)SAM.gov in conjunction with any release into production
- Knowledge-based catalogs of training material

To perform this task, the Contractor shall provide training materials covering all major functionalities that are specific to the audience (e.g. Federal employee, contractor, system integrator, etc.). The contractor shall be responsible for maintaining a comprehensive plan for creating and maintaining training for our stakeholders.

The contractor will ensure all content aligns with the current system functionality. IAE follows the Agile methodology and aims for small and frequent releases of new code to production. This means the self-help materials need to be updated frequently. The contractor shall be given access to the (beta.)SAM.gov content management system to post content onto (beta.)SAM.gov. The contractor will analyze contact issue trends and identify opportunities for self-help materials which could reduce call volume. The contractor may build upon existing materials provided by the government at transition.

4.1.2 Tier 0 Support - All IAE Systems

Contractor shall provide on-line, self-help content to assist system users in performing routine tasks without requiring the assistance from an automated response system or a live customer service representative. System users will access content directly from FSD.gov/(beta.)SAM.gov.

4.1.3 Tier 1 Support – All IAE Systems

Tier 1 is the first call center system directed support point of contact for all customer contacts, Tier 1 provides basic support and troubleshooting, ticket creation, and incident routing, along with escalation to a higher level tier if necessary.

The contractor shall meet this objective by providing first line user assistance and support. This support shall accept service requests through various mediums, and meet the proposed SLAs in satisfying the users' questions and/or issues. This includes, but is not limited to;

- Telephone service requests;

- Web Chat;
- Web-form Service requests;
- Interactive Voice Response (IVR) “Call Back” service requests;
- Email service requests.

The contractor shall provide Tier 1 support and resolve user service requests, such as password resets, general questions, or routine issues that can be diagnosed and resolved without escalation to higher tiers of support in accordance with the service levels proposed.

The contractor shall strive to warm transfer all support between the user, Tier 1 and Tier 2 calls. Only in cases where a live agent is not available in Tier 2 shall the contractor transfer a support call without first briefing the next responder to the circumstances and details of the service request. In cases when a warm transfer is not viable, the contractor shall inform the user, and notify the user of the transfer to a technical team.

The contractor shall prepare for, and adjust to, seasonal changes in customer contact volume. This includes end of federal fiscal year (EOY) increases in demand, as well as historically lower demands early in the federal fiscal year. See Attachment A - FSD Contact Center Data, for historical ticket volume.

At the resolution of a ticket, the contractor shall send a ticket closure email that includes a link to a customer satisfaction online survey. The government will provide to the contractor a “.gov” email for receipt of survey responses. The contractor will route the ticket closure email via the government’s email service to ensure it comes from a ”.gov” domain.

The Contractor shall have the capability to support a wide range of customer service requests types, including, but not limited to:
- Service requests;
- General information requests;
- Referrals;
- Requests on specific programs, applications, and services;
- Emergency requests;
- Complaint requests; and
- Public comments.

All ticket escalation should be noted in the ticket with the specific tier and queue they are being routed to.

4.1.3.1 Phone calls requirements

The contractor shall:
- record all calls, and make them available to the government for their review for ninety (90) days to ensure the government understands the nature of service request calls.
- provide the government the ability to listen in on in-progress calls.
- include a government-provided link to a customer satisfaction survey tool on service request tickets generated. The government will provide

the contractor read-only access to the survey site.
- provide assistance to users in resolving issues and answering questions via phone requests.

4.1.3.2 Real time chat requirements

Contractor shall record all chats with relevant user and agent information and make it available to the government.

4.1.3.3 Web based user interface requirements

The contractor shall provide users with standardized web based request forms. The contractor shall collect relevant information for the request contents and processing and make it available to the government via reports and API.

4.1.4 Limited Tier 2 Support – (beta.)SAM.gov Functionally/ Legacy IAE Systems

The contractor shall provide in a limited capacity, Tier 2 functional support for (beta.)SAM.gov and remaining legacy systems. Tier 2 are second-line responders who have additional expertise or business knowledge, who handle requests unresolved by Tier 1 responders. No Tier 2 functional support is authorized without COR approval. The contractor shall ensure that Tier 2 support is fully capable and enabled of resolving all service requests, unless:

- There are policy, not technology, issues which are the nature of the service request;
- The service request is anticipated to require a change to the system, or application development; or
- The services request requires additional permissions to be granted by the Government.

4.1.4.1 Surge Support

Should a sudden surge (spike) occur in services requests for one or more of the legacy systems or (beta.)SAM.gov functionality, the contractor shall implement, with COR approval, an operational procedure that shifts service request responsibilities to the Tier 1 level.

Under extraordinary circumstances, government approved SLAs may be reduced or suspended with COR and CO approval.

When the contractor has ascertained that the spike has ended, the contractor, with the COR's approval, will return to normal operational procedures in accordance with the provisions of the Tasks identified in this order.

4.2 Technical Objectives

4.2.1 Seamlessly access contact center services from (beta.)SAM.gov

The contractor shall meet this objective by:

- Using login.gov to authenticate customers on fsd.gov.
- Uploading all training (Tier 0) materials to (beta.)SAM.gov via the content management system in accordance with the approved project timeline. Access to the content management system will be provided by the government. All such materials will be approved by the government prior to uploading.
- Updating FSD messages and announcements using the management tool provided by the government. The contractor will provide status to the government if there are outages, maintenance outages or updates to operational status of the FSD so notices can be posted for customer information. All such materials will be approved by the government prior to uploading.
- Providing near real time FSD operational data on (beta.)SAM.gov e.g. wait times, number in queue, alternatives, call back times.
- At a minimum, the following information will be available in (beta.)SAM.gov about the ticket:
    - Customer Name
    - Phone number
    - User email
    - Date ticket created
    - Current system(s) (See Section 1.3)
    - Detailed description of the type of issue as expressed by the user
    - Date ticket closed

4.2.2 Real time data transmission between Contractor and (beta.)SAM.gov

All data is sent in machine readable formats and does not require the government to build custom parsers. The contractor shall meet this objective by complying with the SLAs mutually agreed upon by the contractor and the government. Service Levels Agreements are found in Attachment 7 of the Solicitation – Service Level Agreements.

4.2.3 Meet Service Level Agreements (SLAs)

The contractor shall meet this objective by providing the IAE Team with access to government-approved tools that perform near real time monitoring of the customer experience including government-approved metrics reporting. The tools should be Web based so performance/metrics can be monitored from anywhere. The data available to the IAE team will drive smart, data driven decisions and may include, but not limited to, data such as:

- Average queue time,
- Call length

- Percentage of calls within the SLA
- Number of calls
- Number of active and idle agents
- Calls per minute
- Contact method
- Categories of calls
- Caller profiles
- Calls offered
- Total incidents
- Calls answered
- Average talk time
- Average handle time
- Max delay
- Net abandonment rate
- Chat average wait times
- Phone availability
- First call resolution percentage
- Trends in wait times by day and hour

SLAs will apply only to Tier 1 support. Contractor proposed SLAs will be made a material part of the contract award. Please see Attachment 7 of solicitation - Service Level Agreements. The contractor shall report on progress toward SLAs in monthly reports.

4.2.4 Compliance with IAE design standards

All public facing material needs to meet the IAE design standards detailed in the link provided below.

https://federalist-proxy.app.cloud.gov/site/gsa/sam-styles/

4.2.5 Hard Copy Mail Processing

4.2.5.1 Document Review

The contractor shall provide document review support for various types of documents. Document review will consist of, but not be limited to, the intake of hard copy documents; validation of documents based on government requirements; and government requirements for storage or destruction of documents.

4.2.5.2 Notarized Letter Work

The contractor shall meet this objective by providing notarized letter support for entities appointing and revising Entity Administrators in (beta.)SAM.gov and for new (beta.)SAM.gov registrations and renewals. Contractor will receive instructions from the government (e.g. checklist) to

perform this work for the approval of the Notarized Letter. The performance of this duty will include, but is not limited to,

- receipt of Notarized Letters via postal mail;
- scan letter and envelope;
- generate a service ticket with time stamp;
- attach the Notarized Letter;
- review and verify completeness of Notarized Letter;
- provide associated entity follow up;
- interaction with (beta.)SAM.gov operation contractor;
- electronic storage in contractor's Service Request Management system of all Notarized Letters received by entities currently registered and those seeking to be registered in (beta.)SAM.gov;
- destruction of physical copy of latest version of letter ninety (90) days after digitization.

Notarized Letters will only be required from an entity one time unless there is an Administrator change to the entity. Please see Attachment C - Notarized Letter Processing Data.

4.2.6 Entity Validation Services (EVS)/Unique Entity Identifier (UEI)

Contractor is to provide support to customers contacting the FSD with questions regarding the Entity Validation Services (EVS) and Unique Entity Identifier (UEI).

4.2.6.1 EVS/UEI Purpose

The government has a need for a determination of entity uniqueness to consistently identify specific commercial, nonprofit, or government entities who wish to do business with the federal government. The overarching government requirement is for business identification and validation services. Entity Validation Services are based on federal statute and policy regulations.

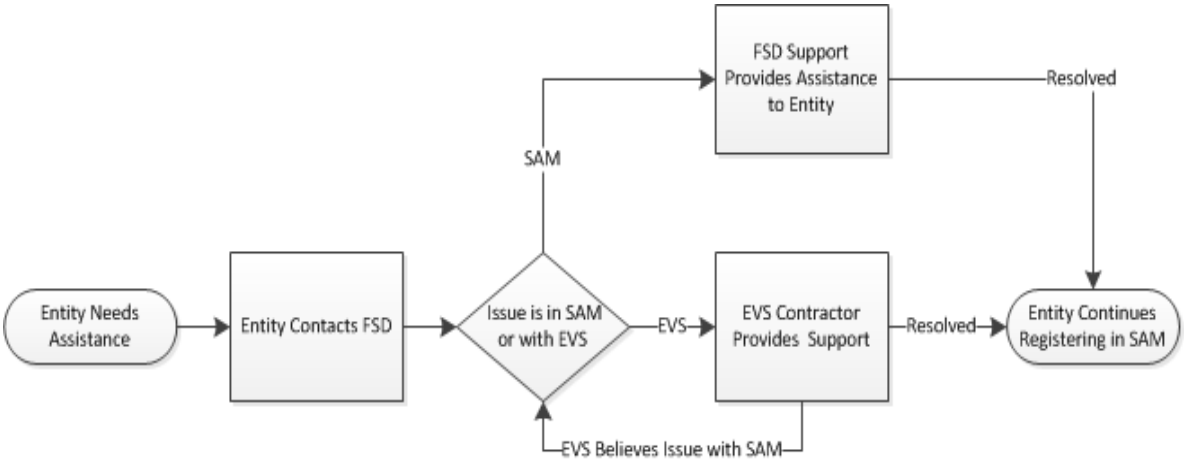
For the purposes of the scope of work for the FSD, FSD should answer questions related to obtaining the UEI, general registration questions, and only refer questions where the registrants information does not match the EVS provider information also referred to as entity data mismatch errors.

4.2.6.2 EVS Customer support capabilities (including entity updates), for U.S. and non-U.S. located entities

Entities, both foreign and domestic, that have validation or identification question about the initial registration data provided to (beta.)SAM.gov that can not be addressed at a Tier 1 level will be escalated to the EVS contractor.

EVS customer support will accommodate entities through multiple communication channels (e.g. phone, internet chat, local offices, email, etc.) with primary support in English and non-English language support if reasonably available, as well as integrate with the FSD ticketing system. This will require communication between the EVS and FSD contractors to ensure seamless delivery of customer services.

Tickets that go beyond the scope of Tier 1 support will be elevated to Tier 2 EVS support and handled by the EVS contractor helpdesk support. An estimated 64,000 tickets/year will be escalated to the EVS contractor helpdesk support and handled by the EVS contractor helpdesk support and not the FSD contractor. All contractors are expected to provide rapid, ready support through multiple communication channels for worldwide registrations.



4.2.7 Integration with IAE Systems

The contractor shall provide any development necessary to provide the services or to facilitate integration with IAE systems, software or interfaces.

4.2.7.1 Integration of Customer Services

When directed by the Government, FSD.gov will be integrated with (beta.)SAM.gov. The contractor shall meet this objective by:

- Providing near real time FSD operational data on (beta.)SAM.gov such as the SLA's outlined in Section 4.2.3. (beta.)SAM.gov will operate data analytics to include FSD activities via the Digital Analytics Program (DAP) that GSA manages government-wide using Google Analytics.
- Ingesting user profiles in login/(beta.)SAM.gov to pre-fill ticket fields for phone calls, pre-populate chats and webforms and capture user input/responses. At a minimum, the following information will be available in (beta.)SAM.gov about the ticket:

  - Customer Name
  - Phone number
  - User email
  - Date ticket created
  - Current system(s) (See Section 1.3)
  - Detailed description of the type of issue as expressed by the user
  - Date ticket closed
- Converting data from a chat tool initiated in (beta.)SAM.gov into a service desk ticket.
- Converting data from webforms completed in (beta.)SAM.gov into a service ticket.
- Enabling the real time viewing of open and historic ticket via the (beta.)SAM.gov work space. The government will develop and manage the workspace pages in (beta.)SAM.gov
- Enabling the real time viewing of service desk performance data via (beta.)SAM.gov
- Enable the use of OAuth.net capabilities to allow single sign-on within the (beta.)SAM.gov environment to access FSD services.

4.2.7.2 Interfaces between Contractor and (beta.)SAM.gov to assign and resolve Tier 2 tickets

The contractor shall build and maintain an interface between their Service Request Ticketing System and (beta).SAM.gov development teams' ticketing system (currently Jira). The interface will facilitate the transmission of Tier 2 technical tickets to the development team's ticketing system and the receipt of status on each ticket back to the contractor Service Request Ticketing System.

GSA, specifically FAS/OSM and GSA IT, reserves the right to change from the current products/tools of Jira/Confluence to another product/tool as business and technical considerations may warrant.

4.2.8 Real Time Electronic Interfaces

The government would prefer to interface with the contractor's system via REST API; however, the contractor may propose alternative transmission methods. Those solution(s) must meet all other business requirements set forth in this PWS and provide timely, accurate, real-time responses. Data transmissions will be transmitted in a manner that is machine readable and simple for the government to parse into (beta.)SAM.gov (e.g. an address shall be broken down into street address, city, state, zip code, country elements and not sent as a single element). All transmission of data, storage of data, and interfacing with GSA systems must be secure and in accordance with all security and data policies set forth in this PWS, based on Federal and GSA security requirements, whenever such requirements are updated.

4.2.9 Batch Transmissions surge

Where the government does not have real time needs, batch transmissions of data are acceptable if these batch transmissions are machine readable and meet all security and data policies set forth in the PWS and solicitation.

4.2.10 Hosting the FSD.gov Site

The contractor shall host the FSD.gov site until such time as the functionality is moved to the (beta.)SAM.gov. The contractor shall complete the following requirements of the FSD.gov site:

- Design should be in line with IAE standards. See Section 4.2.4
- All Tier 0 content shall match the (beta.)SAM.gov most updated learning center materials
- The site will have Chat, Web-form functionality
- The user will be able to see ticket status
- The site will interface with Login.gov to allow for single sign-on;

4.3 Contractor Management Objectives

4.3.1 Continuity of Operations (COOP) support

The contractor shall provide support in a manner that eliminates dependencies on any single call center or geography. In the case of a natural disaster, act of war, act of terrorism, or other act or situation that renders the contractor's call center(s) inoperable, or in the event of a significant unplanned surge of call volumes, the contractor shall have an established and COR approved COOP plan that will provide support with no interruption of service or service levels, IT systems or support, or other operational impact to the Government. The contractor shall have a minimum of one call center and identify the distance from all other facilities. The contractor, with COR approval, can determine that a situation or event has occurred that requires the COOP plan to be executed. When the situation or event has been resolved or remediated, the contractor shall, with COR approval, reconstitute to a non-COOP status.

4.3.2 Program Management

The contractor shall provide program management support under this Task Order. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Performance Work Statement. The contractor shall identify a Senior Project Manager (PM), by name, which shall be approved by the CO in writing, and provide management, direction, administration, quality control, and leadership of the execution of this Task Order. See Section 8 for further information regarding Personnel Qualifications. The contractor shall schedule meetings and provide deliverables in accordance with Sections 5 and 11. All program management activities and hours are to be included in this task, including subtasks, and no program management activities or hours are to be included in any other tasks or subtasks, for the full period of performance of this

order.

4.3.2.1 Project Management Plan (PMP)

The contractor shall document all support requirements in a PMP. The PMP shall:

- Describe the proposed management approach;
- Contain the proposed communication plan;
- Contain the proposed training plan (Section 4.1.2)
- Contain detailed Standard Operating Procedures (SOPs) for all tasks;
- Include milestones, tasks, and subtasks required in this Task Order;
- Provide for an overall Work Breakdown Structure (WBS) and clearly identify who in its organization is responsible for performing each task and also identify situations where responsibility is shared with government partner;
- Include the contractor's final Quality Control Plan (QCP); and proposed detailed SLA's
- Provide a comprehensive Concept of Operations (CONOPS).
- Provide a contingency plan for higher than normal contacts. This is to include emergencies, new policy issues, and known volume increase based on time of year.

4.3.2.2 Update the Project Management Plan (PMP)

The PMP is an evolutionary document that shall be comprehensively updated annually at a minimum. Any major changes in the IAE applications will necessitate a review of the PMP to ensure currency. As the components of the PMP are varied, the contractor may update these sections more frequently as needed and ensure the Government has received a copy of the latest version of the contractor's PMP. The contractor shall work from the latest Government approved version of the PMP.

4.3.2.3 Develop Transition-in Plan

The contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition-in. The attainment of Authority to Operate shall not exceed 180 calendars days after the start date of the Task Order. All transition activities will be completed 180 calendar days after the start date of the Task Order and the contractor shall have the ability to receive and resolve calls within ten (10) calendar days of the receipt of the ATO. Anticipate ninety days to clear personnel en mass. The Government will provide comments on a draft Transition-in Plan at the Kick-off Meeting. The contractor shall provide a final Transition-in Plan within four (4) business days following receipt of Government comments. The transition-in plan shall include, but is not limited to, the following:

- Security clearances of key personnel
- Support government Authority to Operate (ATO) as necessary;
- Provisioning plan and timeline for the Service Request Management System;
- Migration plan to move all open and closed service requests to the Service Request Management System;
- Provisioning plan and timeline for establishing a toll free service phone number;
- Transition on the toll free service phone number;
- IAE subject matter training for the contractor's service desk staff;
- COOP plan, timelines, thresholds, and reconstitution times; and
- API availability for the government to connect Service Management System to (beta.)SAM.gov.

4.3.2.4 Implement the Final Transition-in Plan

The contractor shall implement its Approved Final Transition-in Plan no later than (NLT) 30 calendar days after award.. The contractor shall report weekly on the implementation plan. At a minimum, the Transition Status Report shall include:

- The status of establishing the Service Request Management System;
- The status and progress of transition activities overdue from the prior week's report;
- The planned activities for the prior week;
- The completed activities for the prior week;
- The planned activities for the current week;
- The overall transition status;
- Any issue or task which requires the Government's attention or intervention;
- Assurance all staff have completed appropriate security background investigations before work begins; and
- Knowledge transfer activities between the incumbent contractor and the new contractor.

4.3.2.5 Continual Service Improvement (CSI) Activities

The contractor shall conduct an overall program review, at a minimum on a quarterly basis, and identify where program improvements can be implemented to provide a higher user experience to Government and other users. The contractor shall report this analysis to the Government as part of the Program Improvement Plan. This plan may contain new FAQs or training harvested from User Forum, Blog, or peer-assist activities included in Tier 0-2 support, innovation, technology or changes in business processes within the contractor's direct control, or in associated processes or services. The contractor shall seek to implement these improvements within the scope and ceiling value of the Task Order, with the approval of the contracting officer The contractor shall submit a plan of action to implement these changes to CO and COR and shall attain COR's consent prior to implementing any changes.

4.3.2.6 Transition-out

The Transition-out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to an incoming contractor/Government personnel at the expiration of the Task Order. The contractor shall provide a draft Transition-out Plan 180 Days from Task Order award, and a Final Transition-out Plan NLT 180 calendar days prior to expiration of the Task Order. The contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

- Project management processes
- Points of contact
- Location of technical and project management documentation
- Status of ongoing technical initiatives
- Appropriate contractor–to-contractor coordination to ensure a seamless transition
- Knowledge transfer activities between the incumbent contractor and the new contractor.
- Transition of Key Personnel
- Data Migration Plans
- Schedules and milestones
- Actions required of the Government
- All code developed by the contractor will be considered the property of the US Government.
- Deletion of government data from contractor systems

The contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings.

4.3.3 (beta.)SAM.gov Customer Service Conduct

Customer services in support of this contract are considered to be conducted on behalf of the federal government. Branding, marketing, and sales of the contractor's products or services to callers is strictly prohibited. The contractor may also obtain information regarding entities during customer service support that is not otherwise publicly available. Such data shall not be used for marketing purposes or resale by the contractor while it is not publicly available either through IAE systems or other sources. The contractor is hereby reminded that unauthorized disclosure of non-public information, e.g., proprietary information of third parties, may result in liability under 18 U.S.C. 1905, 18 U.S.C. 1832, or other applicable law.

5. MEETING OBJECTIVES

To accomplish the Meeting Objectives of this Task Order the Contractor shall participate in the following meetings. Nothing discussed in any meetings or discussions between the Government and the Contractor shall be construed as adding, deleting, or modifying

contractual agreement without written authorization from the Contracting Officer.

5.1 Meeting Objective 1 – Initial Business/Kickoff Meeting

Within ten (10) business days following the Task Order award date (or other time mutually agreed between the parties), the Contractor representatives will meet with the GSA Contracting Officer, GSA COR, and Government program manager or designee to review the contractor's understanding of the requirements, goals and objectives of this task order. The contractor shall also address the status of any issues that will affect contractor start-up/ramp-up toward achieving full service/support capability. The Government will be responsible for taking minutes of this meeting. For Deliverables due at the Kick-off Meeting, see Section 11.

5.2 Meeting Objective 2 – Technical Status Meetings

The Contractor shall, participate in technical status meetings approximately three times/week and/or ad hoc technical meetings or ad hoc work status meetings at a mutually agreeable time and place to discuss tasking, SLA metrics performance, work progress, technical problems, performance issues, or other technical matters. During these meetings the Contractor shall at least provide accomplishments, problems and issues and planned actions. The Contractor shall take minutes of these meetings and include them in a Weekly Status Report. These meetings will occur at a time and place mutually agreed upon by the parties.

5.3 Meeting Objective 3 – Monthly Status Meetings

The Contractor shall, if requested by the Government, participate in monthly status meetings at a mutually agreeable time and place to discuss tasking, SLA metrics performance, work progress, technical problems, performance issues, or other technical and operational matters. During these meetings the Contractor shall at least provide accomplishments, problems and issues and planned actions. The Contractor shall take minutes of these meetings and include them in a Monthly Status Report. These meetings will occur at a time and place mutually agreed upon by the parties.

5.4 Meeting Objective 4 – Contract Administration Meetings

The Contracting Officer (CO) may require the authorized Contractor representative to meet or participate in a teleconference with authorized Government personnel as often as deemed necessary to discuss contract performance or administrative issues. The Contractor may also request a meeting with the CO when deemed necessary. The content of meetings shall be documented in writing. Minutes shall be approved by both parties and shall be included in the Government contract file.

6. CONTRACT-WIDE OBJECTIVES

6.1 Contract-wide Objective 1 – Contract and Project Management

The Contractor shall be solely responsible for managing the work performed in the execution of this contract/order. This includes the responsibility to –

- assign appropriate resources to each task,
- maintain clear organizational lines of authority,
- ensure effective contract task management and administration
- establish and use proven policies, processes, analyses, and best practices

The Contractor shall maintain project milestones for each assigned task. The Contractor shall coordinate all work with the FSD Program Office. The Contractor shall update Government representatives on work progress and task milestones during the monthly status meetings.

6.2 Contract-wide Objective 2 – Subcontract Management

The Contractor shall be fully responsible for management, control, and performance of any Subcontractor used on this contract. If a Subcontractor is being used, the Prime Contractor must inform the Government. Use of a Subcontractor on the Contractor's team shall not relieve the Prime Contractor of responsibility, nor accountability, in the execution of this contract/order.

6.3 Contract-wide Objective 3 – Business Relations

A primary element of project success is the business relationship between the Contractor and Government representatives. Within this context the Government will monitor the Contractor's contribution to business relations and provide feedback when required. The Contractor shall make every effort to establish and maintain clear and constant communication channels with the Government primaries (CO, COR, and Government Technical Representative) of this contract for the purpose of:

- Promptly identifying PWS and/or business relationship issues of controversy and the bilateral development and implementation of corrective action plans.
- Ensuring the professional and ethical behavior of Contractor customer support personnel.
- Maintaining effective and responsive Subcontractor management.
- Ensuring the Contractor customer support team is fully aware and engaged in strengthening the interdependence that exists between the Contractors and IAE.
- Facilitating Contractor–Government collaboration for continuous improvement in the conduct of PWS tasks, reducing risks, costs and meeting the mission needs.

6.4 Contract-wide Objective 4 – Contractor Response

The contractor shall ensure prompt response to Government inquiries, requests for information or requests for contractual actions.

6.5 Contract-wide Objective 5 – Team Continuity and Employee Retention

The Government recognizes the benefits in maintaining the continuity of contractor team members. These benefits include but are not limited to retention of corporate knowledge, minimizing contractor customer support familiarization, maintaining/increasing performance levels, schedule adherence and preserving organizational interfaces developed over time. These benefits also accrue to the Contractor. Within the context of effective and efficient personnel management, the Contractor shall take reasonable and

appropriate steps to retain the qualified employees staffed against this contract to maintain continuity and performance while effectively reducing costs borne by the Government. The government is mindful that strong high performing customer support centers cultivate customer service agent retention since it enhances the service quality with experience; high turnover of customer service agents often reduces the quality of service.

6.6 Contract-wide Objective 6 – Professional Appearance

Contractor employees shall present a neat and professional appearance appropriate to the work being performed at all times when interacting with Government representatives, working in Government facilities, or representing the Government at meetings or before third parties.

7. ADDITIONAL PERFORMANCE REQUIREMENTS

7.1 Location of Work

Performance will take place primarily at the contractor's facility. The Project Manager shall be located in the Metropolitan Washington area and will report to the Government site as requested. Other key personnel except the Knowledge Manager shall be Located at the contractor's center of service desk operations for this Task Order.

7.2 Time of Work

7.2.1 Normal Hours

The Federal Service Desk (FSD) which supports the IAE systems is available to users from the hours of 8:00 a.m. to 8:00 p.m. eastern time, Monday through Friday. The contractor shall design their support structure to accommodate the availability of FSD to assist in issue resolution.

For any Contractor employees working on Government facilities, their normal duty hours shall be 8:00 a.m.to 5:00 p.m. PM local time, Monday through Friday, to coordinate with Government operations. The Contractor shall be responsible for managing work hours of its employees, provided they are available when necessary to interact with Government employees. The Contractor may perform work outside the normal duty hours at its own business location(s) or at the Government furnished facilities, when so authorized by CO/COR.

In the event that individual objectives or sub-objectives require expedited performance or extended work days to meet schedule constraints or work volume, the Government shall communicate that need to the Contractor's Project Manager or Team Lead who, in turn, is responsible for managing the Contractor's labor resources to meet the schedule constraints. Communications regarding expedited performance shall be documented in writing and included in the contract administration file. If Contractor employees are working at Government facilities and task completion deadlines require extended hours, the Government will provide authorization to occupy and use Government facilities beyond normal duty hours.

7.2.2 Holidays

Any Contractor employee shall observe federal holidays on the same dates and during the same time as the Government personnel, since Contractor employees shall not have access to the Government facilities during these days and/or times. The Government shall observe the following holidays.

New Years Day	Labor Day
Martin Luther King Jr., Day	Columbus Day
Presidents' Day	Veteran's Day
Memorial Day	Thanksgiving Day
Independence Day	Christmas Day

7.2.3 Government Facility Closures

In the event of unplanned closure of the Government facility for any reason (e.g. natural disasters, government shutdown, or severe weather) the Contractor shall make its best effort to mitigate loss of work time. If Contractor employees are working on the Government installation, this may be done by moving employees to an off-site location. If performance under this contract is not possible, the Contractor shall take steps to assign employees to other projects on a temporary basis or place them in leave status to minimize non-productive costs to the Government under this contract. Additional instructions may be provided by the Contracting Officer on a case-by-case basis. Disagreements between the parties resulting from government closures shall be settled through negotiations to the maximum extent possible or shall otherwise be settled pursuant to the provisions of the Disputes provisions of this contract.

All services to be performed under this contract/order have been determined to be non-essential for performance during a base closure. Should the Government facility be closed, the Contractor shall be notified by either the Contracting Officer, GSA Technical Representative, or a local television or radio station. The Contractor is responsible for notifying its employees about Government closures. Contractor employees are not to report to the Government facility if it is closed and will adhere to delays, unless otherwise specifically instructed otherwise by the CO or GSA Technical Representative.

7.3 Performance at the Contractor's Facilities

The primary Place of Performance is the contractor's facilities. Long distance travel is anticipated to be required in support of this effort, and shall be in performed in accordance with the instructions in Section 7.4, with travel reporting as prescribed in Section 11.9.

The contractor shall have its call center(s) operational and fully staffed (available Monday through Friday, excluding Federal Government Holidays, from 8:00 a.m. Eastern Time to 8:00 p.m. Eastern Time) trained with a Government-approved scripts and be fully transitioned within 180 calendar days of the start of the Task Order. The IVR system shall be used to provide unattended service 24 hours a day, seven days a week.

The contractor's facilities must be in the continental United States.

Work performed at Contractor's work locations shall be performed according to the Contractor's standard commercial practice; however, the Contractor representatives at these locations must be available for interaction with Government employees between the hours of 8:00 a.m. and 8:00 p.m. Eastern time, Monday through Friday, with the exception of government designated holidays or base closures.

7.4 Travel

Travel is anticipated for this task order. The Contractor may be required to travel to any of its customer support (call centers) and Government client locations.

Travel must be coordinated and authorized by the CO, the COR, and/or other identified Government representatives prior to incurring costs. Contractor costs for travel will be reimbursed in accordance with FAR 31.205-46, in arrears. The travel costs shall be reasonable and allowable as defined in FAR 31.201 and in accordance with the limitations of the JTR.

The contractor shall invoice monthly on the basis of cost incurred. The contractor must provide documentation in support of all travel expenses. The contactor will not be reimbursed for local travel (within a 50-mile radius of the Government/contractor's facility) or commuter travel (commute from home to work site).

The contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Long-distance travel shall be scheduled during normal duty hours whenever possible

Invoice submissions including travel costs shall include completed travel expense sheets (i.e., travel voucher) for each trip and each employee who traveled. The travel expense report, receipts of $75 or more (with exceptions being lodging and transportation), and supporting documentation (e.g., approval email for exceeding per diem rates, cost comparisons, etc.) shall be submitted with the invoice. Expense report(s) must include the traveler's name, dates of travel, destination, purpose of travel, Approval Authority documentation (e.g., copy of the e-mail authorizing travel by Government official), and cost for each trip. All travel costs shall be compiled into a travel expense sheet that has been determined to be acceptable by the Government. The entire submission shall be complete and organized to enable the Government to complete an efficient review. Submissions that are not complete and organized are subject to rejection.

7.5 Limitations on Contractor Performance

In compliance with FAR 37.102(c), this task order does not require the contractor to perform any inherently governmental functions. Accordingly, the contractor shall NOT perform any of the inherently governmental functions listed in FAR 7.503. Those inherently governmental functions most applicable to this procurement action are as follows:

- Determine Government policy. [7.503(c)(5)]

- Determine Federal program priorities. [7.503(c)(6)]
- Direct or control Federal employees; [7.503(c)(7)]
- Determine acquisition, disposition, or disposal of Government property; [7.503(c)(11)]
- Determining what supplies or services are to be acquired by the Government [7.503(c)(12)(i)]
- Vote on a source selection board; [7.503(c)(12)(ii)]
- Approve any contractual document on behalf of the Government; [7.503(c)(12)(iii)]
- Award Government contracts; [7.503(c)(12)(iv)]
- Administer Government contracts; [7.503(c)(12)(v)]
- Accept or reject supplies or services; [7.503(c)(12)(v)]
- Terminate Government contracts; [7.503(c)(12)(vi)]
- Determine cost reasonableness, allowability, or allocability; [7.503(c)(12)(vii)]
- Participating as a voting member on performance evaluation boards; [7.503(c)(12)(viii)]
- Determine budget policy, guidance, and strategy [7.503(c)(16)]

7.6 Privacy Act Requirements

Work on this project may require that Contractor personnel have access to information which is subject to the Privacy Act of 1974. Personnel shall adhere to the Privacy act, Title 5 of the U.S. Code, Section 552a and applicable agency rules and regulations when handling this information. Privacy Act information is considered sensitive and appropriate safeguards shall be implemented by the Contractor. The Contractor is responsible for ensuring all contractor personnel are briefed on privacy Act requirements.

7.7 Personal Services

This is not a “Personal Services” contract as defined by FAR 37.104. The government has taken the following steps and precautions to ensure that “Personal Services” employer-employee relationships are not created between government and contractor employees during the performance of this task order. Although Contractor employees who furnish services under this contract are subject to Government technical oversight, the Government shall not oversee Contractor employees but shall provide all direction through the Contractor’s designated representative(s) who is/are solely responsible for supervising and managing Contractor employees. In further compliance with this regulation

- All tasks will be initiated using approved Task Directive Forms.
- All government direction or approval of contractor initiated suggestions shall be documented using approved Task Directive Forms
- All government contract monitors shall communicate with the contractor through the approved contractor management representative.
- All government representatives responsible for managing this task order shall be briefed on the avoidance of personal services and those actions that represent personal services, prior to assuming their contract responsibilities.

7.8 Identification

In compliance with FAR 37.144(c), contractor employees shall avoid creating an

impression in the minds of members of the public or Congress that they are Government officials by taking the following measures.

- All contractor personnel shall be required to wear Government-approved or provided picture identification badges so as to distinguish themselves from Government employees when working at the Government site.
- Additionally, the contractor shall comply with all visitor identification requirements when visiting the Government site.
- When conversing with Government personnel during business meetings, over the telephone or via electronic mail, contractor personnel shall identify themselves as such to avoid situations arising where sensitive topics might be better discussed solely between Government employees.
- Contractors shall identify themselves on any attendance sheet or any coordination documents they may review.
- Electronic mail signature blocks shall identify their company affiliation.
- Where practicable, contractors occupying collocated space with the Government should identify their work space area with their name and company affiliation

7.9 Rehabilitation Act Compliance (Section 508)

Unless otherwise exempt, all services and/or products provided in response to this requirement shall comply with Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d), and the Architectural and Transportation Barriers Compliance Board Electronic and Information Technology (EIT) Accessibility Standards (36 CFR part 1194).

The Contractor shall support the Government in its compliance with Section 508 throughout the development and implementation of the work to be performed. Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d) requires that when Federal agencies develop, procure, maintain, or use electronic information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who do not have disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency. The contractor will be required to perform 508 testing with the use of the most current Job Access With Speech software (JAWS), as we do now with SAM.gov.

Additional information regarding Section 508 can be obtained from the following web sites.

http://www.section508.gov/index.cfm?FuseAction=Content&ID=12
http://www.access-board.gov/508.htm
http://www.w3.org/WAI/Resources

7.10 Avoidance and/or Mitigation of Actual or Potential Organizational Conflicts of Interest

Contractor employees may have access to sensitive government information while performing this work, may be involved in reviewing and assessing the work of other contractors, and may be involved in developing specifications and work statements for subsequent or complementary work.

There is a potential for organizational conflicts of interest if the Contractor has ties with firms whose work it will review or if the Contractor is subsequently awarded a contract that uses a specification or work statement that it prepared. To avoid actual or potential organizational conflicts of interest the Contractor, in conjunction with Government scheduling and oversight controls, must be able to mitigate its relationship with a firm whose work it might review during performance of this Task Order. No specific firm is currently identified but firm may be identified during the course of contract/task order performance.

Additionally, the Contractor shall refrain from seeking contracts that incorporate Contractor generated specifications or work statements until it first demonstrates, to the satisfaction of the Contracting Officer, that obtaining such other contracts will not create an actual or potential organizational conflict of interest with work performed on this task order.

The Contractor shall comply with the provisions of the task order clauses entitled "Organizational Conflicts of Interest," "Notification of Conflicts of Interest Regarding Personnel," "Limitation of Future Contracting," and "Annual Conflict of Interest Certification" to meet this requirement, which shall be incorporated into the Task Order.

8. PERSONNEL REQUIREMENT

NOTE: The Government, at its sole discretion, may consider substitutions and/or requests for deviation from any of the following personnel qualifications (e.g., experience in lieu of education), if to do so would be in the best interest of the Government.

8.1 Personnel Qualifications – General

All personnel working on this contract shall meet the following minimum educational and experience requirements.

- All personnel shall have experience that is appropriate for performing the tasks to which they will be assigned.
- Educational attainment that is appropriate for managing the type of work described in the PWS, both in size and scope.
- An appropriate security clearance as prescribed in Section 9, "Security Requirements" of this PWS.

The Contractor shall furnish adequate documentation to substantiate compliance with this requirement for each assigned staff member. The Contractor shall certify as to the

accuracy and completeness of the supporting documentation.

8.2 Key Personnel

8.2.1 Definition & List of Key Personnel

Key Personnel are defined as those individuals who are so essential to the work being performed that the contractor shall not divert them to other projects or replaced them without receiving prior approval from the Contracting Officer.

The following Contractor personnel will be considered to be “Key Personnel” under this contract / delivery order.

- Senior Program Manager (PM)
- Service Desk Manager
- Knowledge Management Expert
- Senior Training Manager
- Senior Security Officer

All Key Personnel shall comply with all security procedures/requirements within specified time of award.

*Note: Failure of the Contractor to furnish proposed key personnel shall be viewed as a breach of contract and may be grounds for a default determination by the Government.

8.2.1.1 Senior Program Manager (PM)

It is desirable or required as indicated below, that the PM has the following qualifications:

1. Required: Located in the Metropolitan Washington area, and will report to Government site as requested;
2. Required: Experience as a Project Manager or a service desk manager on information technology contracts that include a service desk;
3. Desired: Experience in Communicating with Government personnel, including agency executives;
4. Desired: Experience managing a contract which included a service desk similar in size, scope, and complexity of this Task Order;
5. Desired: Familiarity with the Federal award process:
6. Desired: Familiarity with the Agile development methodology
7. Desired: PMP Certification

8.2.1.2 Service Desk Manager

Is it desirable or required as indicated below, that the Service Desk Manager has the following qualifications:

1. Required: Located at the contractor’s center of service desk operations for this Task Order;
2. Required: Experience managing service center/helpdesk operations

that include a service desk:
3. Desired: Experience in communicating with Government Personnel, including agency executives;
4. Desired: Experience managing a service desk teams supporting the requirements similar in size, scope, and complexity to this Task Order;
5. Desired: Familiarity with the Federal award Process;

8.2.1.3 Knowledge Management Expert

It is desirable or required as indicated below, that the Knowledge Management Expert has the following qualifications;
1. Required: Experience with information Technology contracts that include a service desk;
2. Required: Experience managing knowledge management for a service desk or applications of similar in size, scope, and complexity including internal and external documentation;
3. Desired: Experience communicating with Government Personnel, including agency executives

8.2.1.4 Senior Training Manager

It is desirable or required as indicated below, that the Senior Training Manager has the following qualifications;
1. Required: Located at the contractor's center of service desk operations for this Task Order;
2. Required: Experience with developing user training for information technology contracts;
3. Required: Experience managing training for service desk and external users that is similar in size, scope, and complexity to this Task Order;
4. Desired: Experience communicating with Government Personnel, including agency executives

8.2.1.5 Senior Security Officer

It is desirable or required as indicated below, that the Senior Security Officer has the following qualifications;
1. Required: Experience complying with government security requirements and processes
2. Required: Experience managing security for a government system that is similar in size, scope, and complexity to this Task Order
3. Required: Experience communicating with government security personnel
4. Desired: Certified as a Certified Information Systems Security Professional (CISSP) or equivalent security certification
5. Desired: Experience with Agile Development Methodology

8.2.2 Key Personnel Substitution

If the Government CO and the COR determines that the proposed substitution, or the removal of personnel without substitution or replacement, is unacceptable or would impair the successful performance of the work, the Contracting Officer will

request corrective action. Should the Contractor fail to take necessary and timely corrective action, the Government may exercise its rights under the Disputes provisions of this contract or take other action as authorized under the provisions of this task order, the Prime contract upon which this order is based, or pursue other legal remedies allowable by law.

This includes substitution of those originally proposed at the time of contract/task order award*. Substituted personnel must have equal or better qualifications than the person they replace, subject to the Government's discretion.

The Contractor shall not remove or replace any personnel designated as key personnel without making a written request to and receiving written concurrence from the Contracting Officer. The Contractor's request for a change to key personnel shall be made no later than ten (10) calendar days in advance of any proposed substitution and shall include a justification for the change. The request shall (1) indicate the labor category or labor categories affected by the proposed change, (2) include resume(s) of the proposed substitute in sufficient detail to allow the Government to assess their qualifications and experience, and (3) include a statement addressing the impact of the change on the Contractor performance. Requests for substitution will not be unreasonably withheld by the Government. The Government will approve initial contactor key personnel at the time of award. Replacement key personnel will be approved via modification to the contract/task order.

8.3 Personnel Substitutions

Although Government approval is not required prior to replacing any of its non-key personnel staff, the Contractor shall provide resumes or other adequate documentation to verify to the Government that all proposed replacements (temporary or permanent) meet the security and minimum educational and experience requirements of this PWS. Additionally, the Government requests the courtesy of being immediately informed of any potential vacancy or prior to any staff member being removed, rotated, reassigned, diverted or replaced.

8.4 Staff Maintenance

Due to the demanding nature of this program, it is essential that the Contractor maintain sufficient staffing levels to accomplish all required tasks. This is especially true because many labor skills are in short supply and the program must rely on a single employee to fill one or multiple roles. During any transition of personnel, the Contractor shall make every effort to maintain manning without loss of service days to the Government. This may necessitate the use of temporarily assigned employees to fill short term gaps between permanently assigned employees.

The Contractor is required to use and/or replace all personnel with those who meet the minimum qualifications as stipulated above, in this PWS Section 7 –Personnel Qualifications and Staff Employee Requirements, and should strive to replace departing personnel with those having appropriate and/or equal qualifications. Failure on the part of the Contractor to employ an adequate number of qualified personnel to perform this

work will not excuse the Contractor from failure to perform required tasks within the cost, performance, and delivery parameters of this contract / task order.

8.5 Contractor Employee Work Credentials

Contractors shall ensure their employees and those of their Subcontractors have the proper credentials allowing them to work in the United States. Persons later found to be undocumented or illegal aliens will be remanded to the proper authorities.

9. SECURITY REQUIREMENTS

9.1 Compliance with Security Requirements

The contractor is required to comply with all security regulations and directives as identified herein and other security requirements as are shown elsewhere in this contract. Please refer to the below referenced Security policy documents.

GSA Information Technology (IT) Security Requirements are included in the below Security Policy Documents

- CIO 09-48, IT Security Procedural Guide: Security and Privacy IT Acquisition Requirements
  - https://www.gsa.gov/about-us/organization/office-of-the-chief-information-officer/chief-information-security-officer-ciso/it-security-procedural-guides
- CIO 12-2018, IT Policy Requirements Guide
  - https://www.gsa.gov/cdnstatic/CIO%2012-2018_%20IT%20Policy%20Requirements%20Guide_0.pdf
- CIO IT Security 06-30, Managing Enterprise Risk
  - https://www.gsa.gov/about-us/organization/office-of-the-chief-information-officer/chief-information-security-officer-ciso/it-security-procedural-guides
- DevSecOps OCISO Program [CIO-IT_Security_19-102] [PDF - 806 KB] - 09/13/2019
  - https://www.gsa.gov/about-us/organization/office-of-the-chief-information-officer/chief-information-security-officer-ciso/it-security-procedural-guides

All data should be encrypted in transmission and at rest.

The Contractor shall be responsible for ensuring all employees supporting this contract comply with all security requirements imposed by the Government Security Officer at all times while in Government facilities and shall follow the instructions of the local organization pertaining to security.

The Federal Information Security Modernization Act (FISMA) of 2014 provides a comprehensive framework for ensuring the effectiveness of information security controls across Federal agencies. FISMA focuses on the program management, implementation, and evaluation aspects of the security of federal information systems. It codifies existing security policies, including Office of Management and Budget (OMB) Circular A-130, Revised, and reiterates security responsibilities provided for in the Computer Security Act of 1987, the Paperwork Reduction Act (PRA) of 1995, and the Clinger-Cohen Act (CCA) of 1996.

In order to protect against cybersecurity threats and manage GSA information systems, the Vendor shall ensure that the contract is compliant with Federal security standards and GSA requirements. The Vendor must provide security and protection for information systems that support the operations and assets of the agency, including the support activities provided or managed by a contractor. Relevant areas that GSA's policies address include:

- Security Requirements
- Cloud information system
- Mobile application
- Privacy Protection
- Controlled Unclassified Information
- Incident Reporting Requirements
- Software License Management
- Telecommunications Policy
- Social Media Policy

.

9.1.1 Assessment and Authorization (A&A)

Federal agencies are required by FISMA Law to undergo a security assessment to demonstrate compliance with security requirements. Assessment and Authorizations (A&A) are required for all new systems. The result of a successful A&A is an Authority to Operate (ATO) Memo. The ATO is required before going into operation and processing GSA information system. The failure to obtain/maintain the ATO will result in non-compliance and possible shutdown of the system .

GSA Information Technology IT Security Requirements

The contractor shall deliver an IT Security Plan, as required under CIO 09-48, IT Security Procedural Guide within 30 calendar days of award that describes the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this order. The IT Security Plan shall comply with applicable Federal laws including, but not limited to, 40 U.S.C. 11331, the Federal Information Security Management Act (FISMA) of 2002, and the E-Government Act of 2002. The IT Security Plan shall meet IT security requirements in accordance with Federal and GSA policies and procedures, including General Services Administration Acquisition Regulation (GSAR) clause 552.239-71. The contractor shall submit written proof of IT security authorization six months after award, and verify that the IT Security Plan remains valid annually.·

9.1.2 Recurring Security Deliverables

Deliverables to be provided to the GSA COR/ISSO/ISSM Quarterly

9.1.2.1. Vulnerability Scanning

Reference: NIST 800-53 control RA-5

Provide the most recent Web Application and Operating System

vulnerability scan reports.

9.1.2.2. Plan of Action & Milestones (POA&M) Update

Reference: NIST 800-53 control CA-5
Provide POA&M updates in accordance with requirements and the schedule set forth in GSA CIO IT Security Procedural Guide 09-44, "*Plan of Action and Milestones (POA&M).*"

Deliverables to be provided to the GSA COR/ISSO/ISSM Annually

9.1.3 Updated A&A documentation including the System Security Plan and Contingency Plan

9.1.3.1 System Security Plan

Reference: NIST 800-53 control PL-2
Review and update the System Security Plan annually to ensure the plan is current and accurately describes implemented system controls and reflects changes to the contractor system and its environment of operation. The System Security Plan must be in accordance with NIST 800-18, Revision 1, *"Guide for Developing Security Plans."*

9.1.3.2 Contingency Plan

Reference: NIST 800-53 control CP-2
Provide an annual update to the contingency plan completed in accordance with NIST 800-34, *"Contingency Planning Guide."*

9.1.4. User Certification/Authorization Review Documents

Reference: NIST 800-53 control AC-2
Provide the results of the annual review and validation of system users' accounts to ensure the continued need for system access. The user certification and authorization documents will illustrate the organization establishes, activates, modifies, reviews, disables, and removes information system accounts in accordance with documented account management procedures.

9.1.5 Separation of Duties Matrix

Reference: NIST 800-53 control AC-5
Develop and furnish a separation of duties matrix reflecting proper segregation of duties for IT system maintenance, management, and development processes. The separation of duties matrix will be updated or reviewed on an annual basis.

9.1.6 Information Security Awareness and Training Records

Reference: NIST 800-53 control AT-4
Provide the results of security awareness (AT-2) and role-based information security technical training (AT-3). AT-2 requires basic security awareness training for employees and contractors that support the operation of the contractor system. AT-3 requires information security technical training to information system security roles. Training shall be consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and conducted at least annually.

9.1.7 Annual FISMA Self-Assessment

Reference: NIST 800-53 control CA-2
Deliver the results of the annual FISMA self-assessment conducted per GSA IT Security Procedural Guide 04-26, "*Federal Information Security Modernization Act (FISMA) Implementation."* Based on the controls selected for self-assessment, the GSA OCISO will provide the appropriate test cases for completion.

9.1.8 System(s) Baseline Configuration Standard Document

Reference: NIST 800-53 control CM-2/CM-2(1)
Provide a well-defined, documented, and up-to-date specification to which the information system is built.

9.1.9 System Configuration Settings Verification

Reference: NIST 800-53 control CM-6/CM-6(1)
Establish and document mandatory configuration settings for information technology products employed within the information system that reflect the most restrictive mode consistent with operational requirements. Configuration settings are the configurable security-related parameters of information technology products that compose the information system. Systems should be configured in agreement with GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines in hardening their systems, as deemed appropriate by the Authorizing Official.

Provide the most recent operating system Configuration Settings Compliance scan report.

9.1.10 Configuration Management Plan

Reference: NIST 800-53 control CM-9
Provide an annual update to the Configuration Management Plan for the information system.

9.1.11 Contingency Plan Test Report

Reference: NIST 800-53 control CP-4
Provide a contingency plan test report completed in accordance with GSA IT Security Procedural Guide 06-29, *"Contingency Planning."* A continuity test shall be conducted annually prior to mid-July of each year. The continuity test can be a table top test while the system is at the FIPS PUB 199 Low Impact level. The table top test must include Federal and hosting Contractor representatives. Functional exercises must be completed once every three years for FIPS PUB 199 Moderate impact systems and annually for FIPS PUB 199 High impact systems.

9.1.12 Incident Response Test Report

Reference: NIST 800-53 control IR-3
Provide an incident response plan test report documenting results of incident reporting process per GSA IT Security Procedural Guide 01-02, *"Incident Response."*

9.1.13 Information System Interconnection Agreements

Reference: NIST 800-53 control CA-3
Provide Interconnection Security Agreements (ISA) and supporting Memoranda of Agreement/Understanding (MOA/U), completed in accordance with NIST 800-47, *"Security Guide for Connecting Information Technology Systems,"* for existing and new interconnections. Per NIST 800-47, an interconnection is the direct connection of two or more IT systems for the purpose of sharing data and other information resources through a pipe, such as ISDN, T1, T3, DS3, VPN, etc. ISAs shall be submitted as appendices as part of the annual System Security Plan submission. ISAs shall include, if applicable, any changes since the last submission; updated ISAs are required at least every three years.

9.1.14 Rules of Behavior

Reference: NIST 800-53 control PL-4
Define and establish Rules of Behavior for information system users. Rules of Behavior shall be submitted as an appendix to the System Security Plan.

9.1.15 Penetration Testing Report

Reference: NIST 800-53 control CA-8
All Internet accessible systems, and all FIPS PUB 199 High impact systems are required to complete an independent penetration test and provide a Penetration Test Report documenting the results of the exercise as part of their A&A package. Annual penetration tests are required for these same systems in accordance with GSA Order CIO 2100.1 and CIO-IT Security-11-51, "*Conducting Penetration Test Exercises.*"

9.1.16 Personnel Screening and Security

Reference: NIST 800-53 control PS-3, NIST 800-53 control PS-7
Furnish documentation reflecting favorable adjudication of background investigations for all personnel (including subcontractors) supporting the system. Contractors shall comply with GSA Order CIO 2100.1, *"GSA Information Technology (IT) Security Policy"* and GSA Order, CIO P 2181.1, "*Homeland Security Presidential Directive-12 (HSPD-12) Personal Identity Verification and Credentialing Handbook*." GSA separates the risk levels for personnel working on Federal computer systems into three categories: Low Risk, Moderate Risk, and High Risk.

- Those contract personnel (hereafter known as "Applicant") determined to be in a Low Risk position will require a National Agency Check with Written Inquiries (NACI) investigation.
- Those Applicants determined to be in a Moderate Risk position will require either a Limited Background Investigation (LBI) or a Minimum Background Investigation (MBI) based on the Contracting Officer's (CO) determination.
- Those Applicants determined to be in a High Risk position will require a Background Investigation (BI).

Applicants will not be reinvestigated if a prior favorable adjudication is on file with FPS or GSA, there has been less than a one year break in service, and the

position is identified at the same or lower risk level.

Once a favorable FBI Criminal History Check (Fingerprint Check) has been returned, Applicants may receive a GSA identity credential (if required) and initial access to GSA information systems. The HSPD-12 Handbook contains procedures for obtaining identity credentials and access to GSA information systems as well as procedures to be followed in case of unfavorable adjudications.

Deliverables to be provided to the GSA COR/ISSO/ISSM Biennially

9.1.17 Policies and Procedures

Develop and maintain current the following policies and procedures:
a. Access Control Policy and Procedures (NIST 800-53 AC-1)
b. Security Awareness and Training Policy and Procedures (NIST 800-53 AT-1)
c. Audit and Accountability Policy and Procedures (NIST 800-53 AU-1)
d. Identification and Authentication Policy and Procedures (NIST 800-53 IA-1)
e. Incident Response Policy and Procedures (NIST 800-53 IR-1, reporting timeframes are documented in GSA IT Security Procedural Guide 01-02, "*Incident Response*"
f. System Maintenance Policy and Procedures (NIST 800-53 MA-1)
g. Media Protection Policy and Procedures (NIST 800-53 MP-1)
h. Physical and Environmental Policy and Procedures (NIST 800-53 PE-1)
i. Personnel Security Policy and Procedures (NIST 800-53 PS-1)
j. System and Information Integrity Policy and Procedures (NIST 800-53 SI-1)
k. System and Communication Protection Policy and Procedures (NIST 800-53 SC-1)
l. Key Management Policy (NIST 800-53 SC-12)

9.2 Employee Security Requirements

The contractor shall provide personnel who already have or are capable of attaining and maintaining a Tier 2S security fitness determination. No access will be given to the Government computer information systems and Government sensitive information before the background investigation is completed.

9.2.1 New Contractor Personnel

The full names of all contractor personnel proposed to work under this contract must be submitted to the COR and GSA Security for initiation and/or verification of an individual's security clearance investigation status. No work shall commence under the contract until GSA has received either an initial Enter on Duty Date (EoDD) or a final favorable adjudication and have been approved to work on the contract.

9.2.2 Departing Contractor Personnel

The Contractor shall notify the COR, Contracting Officer and the GSA Personnel Security Officer when Contractor personnel will no longer be working on the contract. The Contractor must then turn in all badges, Government furnished equipment, deliverables and provide an updated listing of GFE.

9.3 Common Access Card & ID Badges

When Government facilities are utilized in the performance of this contract, the Government will provide photo identification, such as Common Access Card (CAC) and Restricted Area Badge (as required). The Contractor shall comply with all requirements necessary to obtain a CAC and Restricted Area Badge.

9.4 Facility Security Requirements

Not Applicable.

9.5 Personal Identity Verification

The Contractor shall comply with the following Personal Identity Verification clause.

FAR 52.204-9, Personal Identity Verification of Contractor Personnel.

(a) The Contractor shall comply with agency personal identity verification procedures identified in the contract that implement Homeland Security Presidential Directive-12 (HSPD-12), Office of Management and Budget (OMB) guidance M-05-24, and Federal Information Processing Standards Publication (FIPS PUB) Number 201.

(b) The Contractor shall insert this clause in all subcontracts when the subcontractor is required to have physical access to a federally-controlled facility or access to a Federal information system.

End of Clause

9.6 Unescorted Entry Authorization Certificate

See the paragraph 9.3 entitled “Common Access Card & ID Badges, “ above.

9.7 Non-Disclosure Statement.

Each Contractor or subcontractor employee (including temporary employees) identified as Key Personnel assigned to work under this contract / order shall complete the attached “Contractor Employee Non-Disclosure Agreement”. A copy of each signed and witnessed Non-Disclosure agreement shall be submitted to the GSA Technical Representative prior to performing any work under this contract.

The Contractor shall not release, publish, or disclose sensitive information to unauthorized personnel, and shall protect such information in accordance with the provisions of the following laws and any other pertinent laws and regulations governing the confidentiality of sensitive information:

18 U.S.C. 641 (Criminal Code: Public Money, Property or Records)
18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information)
Public Law 96-511 (Paperwork Reduction Act)

10. PERIOD OF PERFORMANCE

The maximum potential period of performance of this order is five years starting on the day of Task Order award or designated effective date; with a Base Period of 12 months and four Option Periods of 12 months each. The Government reserves the unilateral right to exercise an option period prior to the expiration of the Base or option period. The Government shall give the Contractor at least 30 days prior notice of its intent to exercise the option.

Planned performance periods are as follows:

Base Period: 5/1/2020 through 4/30/2021
Option 1: 5/1/2021 through 4/30/2022
Option 2: 5/1/2022 through 4/30/2023
Option 3: 5/1/2023 through 4/30/2024
Option 4: 5/1/2024 through 4/302025

11. DELIVERABLES

11.1 Items, Time of Delivery, Place of Delivery

Support services shall be performed to meet a specific task objective. The task objectives and the period of performance shall be stated on individual Task Directives. Task Directives shall include a specific delivery date for reports and studies or a specific completion date for support services. As an alternative, the Task Directives may require the Contractor to establish timelines and milestones for completion of tasks. Government specified delivery or completion dates and Government approval of Contractor proposed timelines or milestones shall be binding on the Contractor. Support services and data items shall be delivered to the Government in compliance with the performance measures and quality requirements set forth in the QASP. All dates are in business days unless otherwise specified.

The Contractor shall deliver the data items listed in the table, below.

CLIN / Ref.	Data Item Title	Delivery Time	Deliver To	Government Data Rights
Section 4.2.8	Real Time Electronic Interfaces and Transmission Methods for Electronic Interfaces (Draft)	Submitted with contractor's quote	As instructed in the solicitation.	Provided with unlimited data rights IAW 52.227-14
Section 4.2.8	Real Time Electronic Interfaces and Transmission Methods for Electronic Interfaces (Final)	Due at Kick off Meeting	Electronically to the GSA ITSS/ASSIST System	Provided with unlimited data rights IAW 52.227-14
Section 4.3.1	COOP Support Plan	Due at Kick off Meeting	Electronically to the GSA ITSS ASSIST System and via email to COR and CO.	Provided with unlimited data rights IAW 52.227-1
Section 4.3.2	Draft Project Management Plan (PMP)	Due at Kick off Meeting	Electronically to the GSA ITSS ASSIST System and via email to COR and CO.	Provided with unlimited data rights IAW 52.227-14
Section 4.3.2	Updated Project Management Plan (PMP)	4 days after receipt of government comments and annually thereafter	Electronically to the GSA ITSS ASSIST System and via email to COR and CO.	Provided with unlimited data rights IAW 52.227-14

Section 4.3.2	Transition-In Plan Draft	Submitted with contractor's quote	Electronically to the GSA ITSS ASSIST System and via email to COR and CO.	Provided with unlimited data rights IAW 52.227-14
Section 4.3.2	Complete Transition-In Plan Draft	With Project Management Plan	Electronically to the GSA ITSS ASSIST System and via email to COR and CO.	Provided with unlimited data rights IAW 52.227-14
Section 4.3.2	Transition-In Plan Final	Due within 4 days after Gov't comments.	Electronically to the GSA ITSS ASSIST System and via email to COR and CO.	Provided with unlimited data rights IAW 52.227-14
Section 4.3.2	Transition Status Report	Weekly, during transition period	Electronically to the GSA ITSS ASSIST System and via email to COR and CO.	Provided with unlimited data rights IAW 52.227-14
Section 4.3.2.6	Continual Service Improvement (CSI)	Quarterly, within 10 days after quarter end.	Electronically to the GSA ITSS ASSIST System and via email to COR and CO.	Provided with unlimited data rights IAW 52.227-14
Section 4.3.2.7	Transition- Out Plan	180 calendar days after TOA.	Electronically to the GSA ITSS ASSIST System via email to COR and CO	Provided with unlimited data rights IAW 52.227-14
Section 4.3.2.7	Transition-Out Plan Updated	180 calendar days prior to the expiration of the order.	Electronically to the GSA ITSS ASSIST System and via email to COR and CO	Provided with unlimited data rights IAW 52.227-14

Section 5.1	Initial Business/ Kickoff Meeting Minutes	No later than 10 days after meeting or as mutually agreed upon	Electronically to the GSA ITSS ASSIST System and via email to COR and CO.	Provided with unlimited data rights IAW 52.227-14
Section 5.2	Technical Status Meetings (Weekly Report)	No later than 3 days after week end	Electronically to the GSA ITSS ASSIST System and via email to COR and CO.	Provided with unlimited data rights IAW 52.227-14
Section 5.3 and 11.7	Monthly Status Report (MSR)	Within 10 days after month end	Electronically to the GSA ITSS ASSIST System and via email to COR and CO.	Provided with unlimited data rights IAW 52.227-14
Section 5.4	Contract Administration Meetings	Within 3 days following each meeting	Electronically to the GSA ITSS ASSIST System and via email to COR and CO.	Provided with unlimited data rights IAW 52.227-14
Section 9.1.1 Security Authorization	Draft Security Plan	Within 30 calendar days after award	Electronically to the GSA ITSS/ASSIST System & email to the IAE COR, PM and CO	Provided with unlimited data rights IAW 52.227-14
Section 9.1.1 Security Authorization	Security Authorization	Within six (6) months after contract award, the Contractor	Electronically to the GSA ITSS ASSIST System and via email to COR, PM and CO.	Provided with unlimited data rights IAW 52.227-14

		shall submit written proof of IT security authorization and all the associated Assessment and Authorization (A&A) documentation for acceptance by the Contracting Officer		
Section 9.1 Security Authorization	Security Authorization	Quarterly Plan Of Actions and Milestones (POA&M) as part of Continuous Security Monitoring	Submit to IAE ISSO IAW GSA Security Policies and Guidelines	Provided with unlimited data rights IAW 52.227-14
Section 9.1 Security Plan	Security Plan Annual Verification	Updated Annually, no later than 10 days after commencement of each option period	Electronically to the GSA ITSS/ASSIST System & email to the IAE COR, PM and CO	Provided with unlimited data rights IAW 52.227-14

Section 9.1.2.1	Vulnerability Scanning	Quarterly, 10 days after each quarter	Electronically to the GSA ITSS ASSIST System and via email to COR and CO, ISSO and ISSM.	Provided with unlimited rights IAW 52.227-14
Section 9.1.2.2.	Plan of Action & Milestones (POA&M) Update	Quarterly, 10 days after each quarter	Electronically to the GSA ITSS ASSIST System and via email to COR and CO, ISSO and ISSM..	Provided with unlimited rights IAW 52.227-14
Section 9.1.3.1	Updated System Security Plan	Annually, 10 days after start of each option period.	Electronically to the GSA ITSS ASSIST System and via email to COR and CO, ISSO and ISSM..	Provided with unlimited rights IAW 52.227-14
Section 9.1.3.2	Updated Contingency Plan	Annually, 10 days after start of each option period.	Electronically to the GSA ITSS ASSIST System and via email to COR and CO, ISSO and ISSM..	Provided with unlimited rights IAW 52.227-14
Section 9.1.4	User Certification/Authorization Review Documents	Annually, 10 days after start of each option period.	Electronically to the GSA ITSS ASSIST System and via email to COR and CO, ISSO and ISSM.	Provided with unlimited rights IAW 52.227-14
Section 9.1.5	Separation of Duties Matrix	Annually, 10 days after start of each option period.	Electronically to the GSA ITSS ASSIST System and via email to COR and CO, ISSO and ISSM.	Provided with unlimited rights IAW 52.227-14

Section 9.1.6	Information Security Awareness and Training Records	Annually, 10 days after start of each option period.	Electronically to the GSA ITSS ASSIST System and via email to COR and CO, ISSO and ISSM.	Provided with unlimited rights IAW 52.227-14
Section 9.1.7	Annual FISMA Self-Assessment	Annually, 10 days after start of each option period.	Electronically to the GSA ITSS ASSIST System and via email to COR and CO, ISSO and ISSM.	Provided with unlimited rights IAW 52.227-14
Section 9.1.8	System(s) Baseline Configuration Standard Document	Annually, 10 days after start of each option period.	Electronically to the GSA ITSS ASSIST System and via email to COR and CO, ISSO and ISSM.	Provided with unlimited rights IAW 52.227-14
Section 9.1.9	System Configuration Settings Verification	Annually, 10 days after start of each option period.	Electronically to the GSA ITSS ASSIST System and via email to COR and CO, ISSO and ISSM.	Provided with unlimited rights IAW 52.227-14
Section 9.1.10	Configuration Management Plan	Annually, 10 days after start of each option period.	Electronically to the GSA ITSS ASSIST System and via email to COR and CO, ISSO and ISSM.	Provided with unlimited rights IAW 52.227-14
Section 9.1.11	Contingency Plan Test Reports	Annually, 10 days after start of each option period.	Electronically to the GSA ITSS ASSIST System and via email to COR and CO, ISSO and ISSM.	Provided with unlimited rights IAW 52.227-14

Section 9.1.12	Incident Response Test Report	Annually, 10 days after start of each option period.	Electronically to the GSA ITSS ASSIST System and via email to COR and CO, ISSO and ISSM.	Provided with unlimited rights IAW 52.227-14
Section 9.1.13	Information System Interconnection Agreements	Annually, 10 days after start of each option period.	Electronically to the GSA ITSS ASSIST System and via email to COR and CO, ISSO and ISSM.	Provided with unlimited rights IAW 52.227-14
Section 9.1.14	Rules of Behavior	Annually, 10 days after start of each option period.	Electronically to the GSA ITSS ASSIST System and via email to COR and CO, ISSO and ISSM.	Provided with unlimited rights IAW 52.227-14
Section 9.1.15	Penetration Testing Report	Annually, 10 days after start of each option period.	Electronically to the GSA ITSS ASSIST System and via email to COR and CO, ISSO and ISSM.	Provided with unlimited rights IAW 52.227-14
Section 9.1.16	Personnel Screening and Security	Annually, 10 days after start of each option period.	Electronically to the GSA ITSS ASSIST System and via email to COR and CO, ISSO and ISSM.	Provided with unlimited rights IAW 52.227-14
Section 9.1.17	Policies and Procedures	Biennially, 10 days after start of each alternating option period.	Electronically to the GSA ITSS ASSIST System and via email to COR and CO, ISSO and ISSM.	Provided with unlimited rights IAW 52.227-14

Section 11.3 and 9.7	Contractor Employee Non-disclosure Agreement (NDA)	Prior to commencement of performance by each Contractor or Subcontractor employee	Electronically to the GSA ITSS ASSIST System and via email to COR and CO.	Provided with unlimited data rights IAW 52.227-14
Section 11.5	Staff Plan (Draft)	Submitted with contractor's quote	Electronically to the GSA ITSS ASSIST System and via email to COR and CO.	Provided with unlimited data rights IAW 52.227-14
Section 11.5	Staffing Plan (Final)	Kick off meeting and within 10 days of each quarter end	Electronically to the GSA ITSS ASSIST System and via email to COR and CO.	Provided with unlimited data rights IAW 52.227-14
Section 11.8	Trip Report	5 business days after trip completion.	Electronically to the GSA ITSS ASSIST System and via email to COR and CO.	Provided with unlimited data rights IAW 52.227-14

Section 11.6	Funds and Man-Hour Expenditure Report	Submitted with Monthly Status Report, within 10 business days after month end.	Electronically to the GSA ITSS ASSIST System and via email to COR and CO.	Provided with unlimited data rights IAW 52.227-14
Section 12	Quality Control Plan Draft	30 days after award of TO	n/a	Provided with unlimited rights IAW 52.227-14
Section 12	Quality Control Plan Final	10 days after receipt of government comments	Electronically to the GSA ITSS ASSIST System and via email to COR and CO.	Provided with unlimited rights IAW 52.227-14

11.2 Data Requirements / Descriptions /Markings

Documentation provided in response to the objectives will be in the Government's template format. If no format is prescribed, documents may be in the Contractor's preferred format using standard Microsoft Office products or in PDFs.

The content of all data items, if not self-explanatory from the template format, shall be agreed upon between the parties.

The contractor shall provide all materials and deliverables free of markings, to include, but not limited to, intellectual property claims/markings, copyright claims/markings, or corporate proprietary claims/markings. The contractor can provide a deliverable document to the Contracting Officer and the COR with proposed markings. The Contracting Officer will consider the request and approve or deny the request.

When requesting marking on deliverables, the contractor shall provide the above submission 3 business days prior to the deliverable due date. No allowances or consideration will be given to the contractor should it fail to provide such notice.

11.3 Contractor Employee Non-Disclosure Agreement

The Contractor shall furnish a signed "Contractor Employee Non-Disclosure Agreement" for each Contractor and Subcontractor employee assigned to work under this contract / order, prior to their starting work. Please see Attachment D – Contractor Employee

Non-Disclosure Agreement.

11.4 Quality Control Plan

The Contractor shall deliver a QCP as defined in Section 12.1 of this PWS.

11.5 Staff Plan

The Contractor shall furnish a complete and current list of Contractor and Subcontractor Customer support employees who are assigned to work under this contract / order. The plan shall include the staffing chart showing the name of each employee, his or her position in the staffing plan, job title, and the Government's task/office/function they are supporting. If the names of non-key personnel are not known prior to the quote submission, the offeror may indicate "TBD" in place of the name of each employee in the draft project staffing plan. The lines of authority and responsibility of each staff member shall also be made clear to the Government. The plan shall be updated with each change in personnel, job title, position in the staffing plan, or assignment of area of responsibility.

11.6 Funds and Man-Hour Expenditure Report

The contractor shall provide a Funds and Man-Hour Expenditure Report that provides the current task order accounting information indicated below. The Contractor can determine the format of the report provided it includes, at a minimum, the following information:

- Expenditures for labor, material, travel, and any other charges.
- Matrix of Actual hours expended vs. planned and/or funded hours, and an explanation of significant variances between planned and expended hours. The report shall include amounts for the current monthly reporting period and the cumulative actual vs. planned hours and amounts for the entire contract/order up to the report date.
- Burn rates for the current period and the cumulative amount for the entire contract/order up to the report date. The information shall be presented in numerical and chart format for each CLIN
- Crosswalk of work performed to amounts billed.

In addition, the Funds and Man-Hour Expenditure Report shall include labor charges for actual hours worked and Support Items, which are authorized in the task (e.g., travel, training, etc.). Charges shall not exceed the authorized cost limits established for labor and Support Items. The government will not pay any unauthorized charges. Original receipts, travel vouchers, etc. completed in accordance with government Travel Regulations shall be maintained by the contractor to support charges other than labor hours and made available to government auditors upon request.

11.7 Monthly Status Report (MSR)

The contractor shall provide a MSR that briefly summarizes, by task, the management and technical work conducted during the month, as well as business information listed in the Section 11 Deliverables. The contractor shall provide at a minimum the following information:

- Summary of effort, progress and status of all activities/requirements by task linked to deliverables as appropriate
- New work added since the previous Monthly Status Meeting
- Brief summary of activity planned for the next reporting period
- Deliverables submitted for the period by task and linked to the milestone schedule
- All standards followed in support of the requirements
- Staffing
- Milestone updates and schedule changes, issues and/or variances.
- Problems or issues and SLA data metrics.
- Number of notarized letters processed and related statistics such as # rejected, resubmitted, etc.
- Government action requested or required

11.8 Security Deliverables

Deliverables to be provided to the GSA COR/ISSO/ISSM Quarterly

11.8.1. Vulnerability Scanning

Reference: NIST 800-53 control RA-5
Provide the most recent Web Application and Operating System vulnerability scan reports.

11.8.2. Plan of Action & Milestones (POA&M) Update

Reference: NIST 800-53 control CA-5
Provide POA&M updates in accordance with requirements and the schedule set forth in GSA CIO IT Security Procedural Guide 09-44, "*Plan of Action and Milestones (POA&M)*."

Deliverables to be provided to the GSA COR/ISSO/ISSM Annually

11.8.3 Updated A&A documentation including the System Security Plan and Contingency Plan

11.8.3.1. System Security Plan

Reference: NIST 800-53 control PL-2
Review and update the System Security Plan annually to ensure the plan is current and accurately describes implemented system controls and reflects changes to the contractor system and its environment of operation. The System Security Plan must be in accordance with NIST 800-18, Revision 1, *"Guide for Developing Security Plans."*

11.8.3.2. Contingency Plan

Reference: NIST 800-53 control CP-2
Provide an annual update to the contingency plan completed in accordance with NIST 800-34, *"Contingency Planning Guide."*

11.8.4. User Certification/Authorization Review Documents

Reference: NIST 800-53 control AC-2
Provide the results of the annual review and validation of system users' accounts to

ensure the continued need for system access. The user certification and authorization documents will illustrate the organization establishes, activates, modifies, reviews, disables, and removes information system accounts in accordance with documented account management procedures.

11.8.5. Separation of Duties Matrix

Reference: NIST 800-53 control AC-5
Develop and furnish a separation of duties matrix reflecting proper segregation of duties for IT system maintenance, management, and development processes. The separation of duties matrix will be updated or reviewed on an annual basis.

11.8.6. Information Security Awareness and Training Records

Reference: NIST 800-53 control AT-4
Provide the results of security awareness (AT-2) and role-based information security technical training (AT-3). AT-2 requires basic security awareness training for employees and contractors that support the operation of the contractor system. AT-3 requires information security technical training to information system security roles. Training shall be consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and conducted at least annually.

11.8.7. Annual FISMA Self-Assessment

Reference: NIST 800-53 control CA-2
Deliver the results of the annual FISMA self-assessment conducted per GSA IT Security Procedural Guide 04-26, "*Federal Information Security Modernization Act (FISMA) Implementation."* Based on the controls selected for self-assessment, the GSA OCISO will provide the appropriate test cases for completion.

11.8.8. System(s) Baseline Configuration Standard Document

Reference: NIST 800-53 control CM-2/CM-2(1)
Provide a well-defined, documented, and up-to-date specification to which the information system is built.

11.8.9 System Configuration Settings Verification

Reference: NIST 800-53 control CM-6/CM-6(1)
Establish and document mandatory configuration settings for information technology products employed within the information system that reflect the most restrictive mode consistent with operational requirements. Configuration settings are the configurable security-related parameters of information technology products that compose the information system. Systems should be configured in agreement with GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines in hardening their systems, as deemed appropriate by the Authorizing Official.

Provide the most recent operating system Configuration Settings Compliance scan report.

11.8.10. Configuration Management Plan

Reference: NIST 800-53 control CM-9
Provide an annual update to the Configuration Management Plan for the information system.

11.8.9. Contingency Plan Test Report

Reference: NIST 800-53 control CP-4
Provide a contingency plan test report completed in accordance with GSA IT Security Procedural Guide 06-29, *"Contingency Planning."* A continuity test shall be conducted annually prior to mid-July of each year. The continuity test can be a table top test while the system is at the FIPS PUB 199 Low Impact level. The table top test must include Federal and hosting Contractor representatives. Functional exercises must be completed once every three years for FIPS PUB 199 Moderate impact systems and annually for FIPS PUB 199 High impact systems.

11.8.10. Incident Response Test Report

Reference: NIST 800-53 control IR-3
Provide an incident response plan test report documenting results of incident reporting process per GSA IT Security Procedural Guide 01-02, *"Incident Response."*

11.8.11 Information System Interconnection Agreements

Reference: NIST 800-53 control CA-3
Provide Interconnection Security Agreements (ISA) and supporting Memoranda of Agreement/Understanding (MOA/U), completed in accordance with NIST 800-47, *"Security Guide for Connecting Information Technology Systems,"* for existing and new interconnections. Per NIST 800-47, an interconnection is the direct connection of two or more IT systems for the purpose of sharing data and other information resources through a pipe, such as ISDN, T1, T3, DS3, VPN, etc. ISAs shall be submitted as appendices as part of the annual System Security Plan submission. ISAs shall include, if applicable, any changes since the last submission; updated ISAs are required at least every three years.

11.8.12. Rules of Behavior

Reference: NIST 800-53 control PL-4
Define and establish Rules of Behavior for information system users. Rules of Behavior shall be submitted as an appendix to the System Security Plan.

11.8.13. Penetration Testing Report

Reference: NIST 800-53 control CA-8
All Internet accessible systems, and all FIPS PUB 199 High impact systems are required to complete an independent penetration test and provide a Penetration Test Report documenting the results of the exercise as part of their A&A package. Annual penetration tests are required for these same systems in accordance with GSA Order CIO 2100.1 and CIO-IT Security-11-51, "*Conducting Penetration Test Exercises.*"

11.8.14. Personnel Screening and Security

Reference: NIST 800-53 control PS-3, NIST 800-53 control PS-7
Furnish documentation reflecting favorable adjudication of background investigations for all personnel (including subcontractors) supporting the system. Contractors shall comply

with GSA Order CIO 2100.1, *"GSA Information Technology (IT) Security Policy"* and GSA Order, CIO P 2181.1, "*Homeland Security Presidential Directive-12 (HSPD-12) Personal Identity Verification and Credentialing Handbook*." GSA separates the risk levels for personnel working on Federal computer systems into three categories: Low Risk, Moderate Risk, and High Risk.

- Those contract personnel (hereafter known as "Applicant") determined to be in a Low Risk position will require a National Agency Check with Written Inquiries (NACI) investigation.
- Those Applicants determined to be in a Moderate Risk position will require either a Limited Background Investigation (LBI) or a Minimum Background Investigation (MBI) based on the Contracting Officer's (CO) determination.
- Those Applicants determined to be in a High Risk position will require a Background Investigation (BI).

Applicants will not be reinvestigated if a prior favorable adjudication is on file with FPS or GSA, there has been less than a one year break in service, and the position is identified at the same or lower risk level.

Once a favorable FBI Criminal History Check (Fingerprint Check) has been returned, Applicants may receive a GSA identity credential (if required) and initial access to GSA information systems. The HSPD-12 Handbook contains procedures for obtaining identity credentials and access to GSA information systems as well as procedures to be followed in case of unfavorable adjudications.

Deliverables to be provided to the GSA COR/ISSO/ISSM Biennially

11.8.15. Policies and Procedures

Develop and maintain current the following policies and procedures:

a. Access Control Policy and Procedures (NIST 800-53 AC-1)
b. Security Awareness and Training Policy and Procedures (NIST 800-53 AT-1)
c. Audit and Accountability Policy and Procedures (NIST 800-53 AU-1)
d. Identification and Authentication Policy and Procedures (NIST 800-53 IA-1)
e. Incident Response Policy and Procedures (NIST 800-53 IR-1, reporting timeframes are documented in GSA IT Security Procedural Guide 01-02, "*Incident Response*"
f. System Maintenance Policy and Procedures (NIST 800-53 MA-1)
g. Media Protection Policy and Procedures (NIST 800-53 MP-1)
h. Physical and Environmental Policy and Procedures (NIST 800-53 PE-1)
i. Personnel Security Policy and Procedures (NIST 800-53 PS-1)
j. System and Information Integrity Policy and Procedures (NIST 800-53 SI-1)
k. System and Communication Protection Policy and Procedures (NIST 800-53 SC-1)
l. Key Management Policy (NIST 800-53 SC-12)

11.9 Travel Expense Reports

For all long distance travel, the contractor shall submit Travel Expense Reports five working days after completion of a trip. (See Section 4). Local travel within 50 miles of government facility is not subject to reimbursement.

The Trip Report shall include the following information:

- Personnel traveled
- Dates of travel
- Destination(s)
- Purpose of Trip; Task objective supported; (if applicable); training (be specific)
- Actual Trip Costs (See Joint travel regulation for list of approved costs)
- Approval Authority (Copy of the e-mail or Travel Authorization Request authorizing travel by Government official)
- Summary of trip events and accomplishments

The contractor shall reconcile the Trip Reports with each invoice such that they can be matched month by month.

11.10 Other Reports

Content of other reports is self-explanatory or as further detailed in this section.

11.12 Transition-in

Transition-in will be signified by the following monthly deliverables

• Complete Transition-In Plan Draft (PWS 4.3.2)	June
• Draft Project Management Plan (PWS 4.3.2) inclusive of: – Communication Plan – Training Plan – Integrated Master Schedule with Milestones, Tasks, and Subtasks – Work Breakdown Structure – Final Quality Control Plan ▪ Service Level Agreements – Concept of Operations (PWS 4.3.1) – Contingency Plan for Surges • Staffing Plan • Real time Electronic Interfaces and Transmission Methods (PWS 4.2.8) Continuity of Operations Plan • Final Transition-In Plan (PWS 4.3.2) • Transition Plan and Schedule for Incumbent Knowledge Transfer • Draft Security Plan (PWS 9.1.1)	July
• Knowledge Transfer Complete and Documented • Standard Operating Procedures (PWS 4.3.2)	August
• Contact Center Operations Environment Design, Development, Testing – Agent desktops and facility preparation – Contact Center Tools such as ITSM and ACDaaS	September

• Recruiting and Hiring (including security clearance paperwork) • Tier 1 Training Materials • Tier 0 Materials/Content • Training of Tier 1 Supervisors • Tier 2 Train-the-Trainer	October
• Training of Tier 1 and Tier 2 Agents • ATO Received • FSD.gov hosted • Transition Complete	November

12. QUALITY ASSURANCE AND QUALITY CONTROL

12.1 Contractor Quality Control Plan (QCP)

The Contractor shall be responsible for quality assurance and quality control of all services performed and all items delivered under this contract/order.

The Contractor shall prepare and maintain a Quality Control Plan (QCP) as a guide for implementing quality assurance and quality control procedures. The Contractor shall submit the QCP to the Government for information and acceptance. The Government has the right to require revision of the Contractor's QCP should its implementation fail to control the quality of items and/or services delivered under this contract/order.

The QCP shall include an explanation of the processes and procedures for ensuring satisfactory performance and delivery of quality items and/or services. Additionally, as a minimum, the QCP shall include the following items:

- A description of the inspection system to cover all major services and deliverables. The description shall include specifics as to the areas to be inspected on both a scheduled and unscheduled basis, frequency of inspections, and the title of inspectors.
- A description of the methods to be used for identifying and preventing defects and deficiencies in the quality of service performed.
- A description of the records to be kept to document inspections and corrective or preventive actions taken.

All records of inspections performed shall be retained and made available to the Government upon request throughout the task order performance period, and for the period after task order completion, until final settlement of any claims under this task order.

The Contractor shall implement a quality program based on its QCP. In compliance with the QCP, the Contractor shall manage, surveil, assess, improve and/or correct contract performance to ensure the quality of the services and deliverable products, as a minimum, meet the level of quality required by the Government Functional Managers or Technical Representatives.

In the event of quality concerns, identified by the Government, the Contractor shall immediately take corrective action in response to Government required changes to the QCP.

The QCP shall be delivered to the Government as stipulated in the Delivery Schedule, see Paragraph 6.1 of this PWS, above.

12.2 Government Quality Assurance Surveillance Plan (QASP)

The Government will evaluate Contractor's performance under this contract / task order in accordance with the attached Quality Assurance Surveillance Plan (QASP). The purpose of this evaluation is to ensure that Contractor performance meets Government requirements. The QASP also indicates the potential decrease in compensation for unsatisfactory performance due to a reduction in value received. The Government reserves the unilateral right to change the QASP at anytime during contract performance provided the changes are communicated to the Contractor by the effective date of the change. The QASP along with its attached “Surveillance Objectives, Measures, and Expectations” and “Performance Evaluation” chart identifies evaluation procedures, PWS items to be evaluated, and the measures against which performance will be evaluated. The QASP is provided as Attachment E of this PWS.

13. GOVERNMENT FURNISHED ITEMS

The Government will provide the following resources to the Contractor for task performance:

13.1 Data

The Government will provide documents reports, database access, .gov survey email address, data, and other information as available and as required to facilitate the accomplishment of work as stated within this PWS. The contractor may build upon existing materials to be provided, such as:

- Frequently Asked Questions (FAQs);
- Webinars
- Announcements and change notices
- Pre-recorded demonstrative videos
- Articles on specific tasks or processes

Government Furnished Information shall include: Federal Service Desk Call Scripts, Frequently Asked Questions located at www.fsd.gov and historical ticketing data.

The contractor is responsible for obtaining data necessary to perform each task if that data is in the public domain and is not otherwise furnished by the government.

13.2 Equipment – Tools – Accessories

Except as indicated under 13.5 below, no Government facilities or IT Equipment will be provided to the contractor under this order.

When Government facilities are utilized in the performance of this contract, the Government will provide the standard desktop configuration office equipment (office

work area, desks, chairs, file space, lighting, telephones, access to fax, computers, software, network access, general office supplies, etc.) The Government will provide a desktop computer and email account. The Government will provide telephone service for official use. The Government will pay for all official commercial long distance calls, from Contractor duty station, made in the performance of this contract.

The Contractor shall immediately terminate Government LAN access and/or transfer LAN access responsibility for any employee terminated or transferred from this contract. This is a condition of GFP, if applicable.

13.3 Materials

Not applicable to this contract/order.

13.4 Government Furnished Information

Please see Section 13.1

13.5 Facilities

From time to time, as dictated by task requirements, one or two Contractor employees may be required to work at the Government facilities. The Government will provide office space for these employees, when required.

When Government facilities are utilized in the performance of this contract, the Government will provide photo identification (See Paragraph 9 Security Requirements)

NOTE: All Government-provided products and facilities remain the property of the Government and shall be returned upon completion of the support services. Contractor personnel supporting this requirement shall return all items that were used during the performance of these requirements by the end of the performance period.

13.6 Safeguarding Government Furnished Property - Physical Security

The Contractor shall be responsible for safeguarding all Government property provided for Contractor use. At the end of each work period, Government facilities, property, equipment and materials shall be secured. The Contractor shall be responsible for any damage caused by his personnel to the building, finishes, furnishings, equipment, etc., and shall repair, clean, replace, or restore damaged items to the condition existing immediately prior to the item being damaged.

13.7 Training

During the course of this contract / order the Government may require Contractor employees to receive specialized training in areas necessary to allow the Contractor to fulfill the requirements of this contract / order (e.g., LAN Information Assurance Training, Government unique software or software tools, Security Training). In such cases Government mandated training shall be considered part of this contract and charged against the task(s) to which the individual Contractor employee is assigned.

NOTE: *The Contractor shall be responsible for the supervision, training and guidance of its personnel to accomplish this contract / order. Unless Contractor employee training is specifically identified and authorized by the Government, in writing, the Contractor shall not bill the Government for employee time spent in training or for any costs related to or associated with Contractor employee acquired training. This applies to training of any type or for any purpose, including training that is either necessary for job or employment eligibility or a prerequisite to performance of work under this contract/order, whether general in nature or specialized and unique to this requirement.*

13.8 Government-Furnish Services

Not Applicable

14. GOVERNMENT DELAYS IN REVIEWING DELIVERABLES OR FURNISHING ITEMS

If contractor performance or submission of deliverables is contingent upon receipt of government furnished items (data, equipment, materials, facilities, and support) or input, or upon government review and approval of interim items or draft documents (collectively referred to as Government Performance), the government shall specify when it will provide such items or input, or the time it will need to perform reviews or give approvals. If the government fails to meet item, input, review, or approval deadlines, contractor performance or submission of deliverables shall automatically be extended one calendar day for each day of government delay. The contractor shall promptly advise the Contracting Officer of any delays in receipt of government furnished items, input, reviews, or approvals. If dates for Government performance are not specified in this contract/order or associated task directives, this clause will not apply, and contractor delays must be handled or negotiated under other provisions of this contract or order.

15. NOTICES

15.1 Contracting Officer's Representative

The work to be performed under this contract is subject to monitoring by an assigned Contracting Officer Representative (COR). The COR appointment letter, outlining the COR responsibilities under this contract/order, will be provided to the contractor under separate cover upon request. Questions concerning COR appointments should be addressed to the Contracting Officer.

15.2 Government Technical Representative - Task Management

In addition to the COR, the Government will assign one or more project/program managers to manage and monitor the work under this contract / task order. One of these individuals may be assigned as the Government Technical Representative. The Government Technical Representative will participate in project meetings and review task order deliverables and will provide technical assistance and clarification required for the performance of this task. Refer to the attached QASP for specific information on

project monitoring.

16. CONTACT INFORMATION

16.1 Contractor Contacts

[To be added at time of contract award.]

16.2 Government Contacts:

GSA Federal Acquisition Service

Primary Contracting Officer
Ms. Julie Green
230 South Dearborn Street, 33rd Floor
Chicago, Illinois 60604
Phone: 312 / 353-7036
Fax: 312 / 886-3827
email: julie.green@gsa.gov

Alternate Contracting Officer
Mr. Eben Greybourne
230 South Dearborn Street, 33rd Floor
Chicago, Illinois 60604
Phone: 312 / 886-3811
Fax: 312 / 886-3827
email: eben.greybourne@gsa.gov

Primary – IAE
Mr. Gregory Sizemore GSA
Current FSD Project Manager
1800 F Street NW
Washington, DC 20405
Phone: 703 / 969-4977
Email: greg.sizemore@gsa.gov

Ms. Karen Poole
New FSD Project Manager
2300 Main Street, 2NE
Kansas City, MO 64108
Phone: 312 / 886-3811
email: karen.poole@gsa.gov

Alternate – IAE COR (current & new FSD; main POC)
Anthony Melia
Assistant Project Manager
1800 F Street NW
Washington, DC 20405
Email: anthony.melia@gsa.gov

17. ADDITIONAL PROVISIONS

17.1 Data Rights

The Government shall have unlimited royalty free rights to all data originally developed, generated and delivered under this contract or order as prescribed by the clause entitled **Rights in Data—General** (FAR 52.227-14 **)** which is incorporated into this task order contract. The Contractor shall retain all rights to data used to meet the requirements of this task order if developed solely at the Contractor's expense for their commercial applications and sales.

The Government shall have the right to use all commercially developed and privately funded data delivered under this contract or order in accordance with, and subject to, the published agreements and restrictions that accompany that data.

17.2 Limited Use of Data

All data delivered or made available to the Contractor as Government Furnished Data shall remain the property of the Government and shall only be used by the Contractor in the performance of this contract or order. The Government retains all rights to Government Furnished Data.

At the conclusion of this contract/order all Government Furnished Data shall be dealt with according to the disposition instruction provided by the Contracting Officer. If the Contracting Officer fails to provide disposition instructions for Government Furnished Data within thirty days of contract/task order end, the Contractor shall return all hard copy data and delete or otherwise destroy all electronic data.

17.3 Proprietary Data

The Contractor shall not employ the use of any proprietary data or software in the performance of this contract without the advanced written consent of the Contracting Officer.

17.4 Inspection and Acceptance

All deliverables will be inspected for content, completeness, accuracy and conformance to TO requirements by the COR. Inspection may include validation of information or software through the use of automated tools, testing or inspection of deliverables as specified in the TO. The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality and adequacy of all deliverables.

Inspection and acceptance will occur in accordance with the clause entitled Inspection of Services – Time and Material and Labor Hour (FAR 52.246-6) or Inspection of Services – Fixed Price (FAR 52.246-4), as applicable. In the absence of other agreements negotiated with respect to time provided for government review, deliverables will be inspected and the contractor notified of the COR's findings within fifteen (15) work days of normally scheduled review. Unacceptable or unsatisfactory work will be handled as outlined in the QASP. Acceptance of invoices shall constitute acceptance of performance.

Inspection and acceptance shall be at destination.

17.5 Contract Type

This task order/contract will be awarded using a combination Firm Fixed Price/Time & Material contract type.

17.6 Ceiling Price Notification

Per clause 52.323-7(d), Payments under Time-and-Materials and Labor-Hour Contracts,

the contractor is reminded – “If at any time the Contractor has reason to believe that the hourly rate payments and travel costs that will accrue in performing this contract in the next succeeding 30 days, if added to all other payments and costs previously accrued, will exceed 85 percent of the ceiling price in the Schedule, the Contractor shall notify the Contracting Officer giving a revised estimate of the total price to the Government for performing this contract with supporting reasons and documentation.”

17.7 Task Order Funding

It is anticipated that the task order will be incrementally funded. Accordingly, the following provision applies.

17.8 Incremental Funding

If the contract will be incrementally funded, the appropriate funding clause(s) will be included in the award document.

17.9 Material and Material Handling Costs

Material and material handling costs will be paid as provided in FAR 52.232-7(b) “Payments under Time-and-Materials and Labor-Hour Contracts”. Allocable indirect costs (e.g. Material overhead) will not be authorized if the costs are included in the hourly rate. The Government will not pay profit or fee on materials.

17.10 Productive Direct Labor Hours

The Contractor shall only charge for labor hours when work is actually being performed in connection with this Task Order and not for employees in a “ready” status only. For this task order 1 FTE (full time equivalent) = 1960 labor hours.

17.11 Invoicing and Payment

The following provision applies to the fixed price supply or fixed price services portion of this task order and is incorporated into this order by reference - FAR 52.232-1, Payments (Apr 1984)

The following provision applies to the time and material or labor hour portion of this task order and is incorporated into this order by reference - FAR 52.232-7, Payments under Time-and-Materials and Labor-Hour Contracts

The Contractor may invoice for items upon their delivery or services when rendered. Billing and payment shall be accomplished in accordance with contract terms and GSA payment procedures. The invoice shall reflect the complete project or item charges. The Contractor shall submit invoices and supporting documents through ITSS for Government review and certification that delivered items or services have been received and are acceptable. The GSA payments office considers items and/or services approved for payment upon electronic acceptance through the ITSS system by the Government office designated for receipt of the items and/or services. The Contractor must also submit invoices directly to the GSA payment office electronically. Complete instructions will be provided with the award document. Should the Contractor desire an advanced

copy of the complete GSA payment instructions it may be obtained by contacting the Contracting Officer. Electronic acceptance by the Government Technical Representative is considered concurrence and acceptance of products.

17.12 Payment for Unauthorized Work

The Contractor will not be paid for the performance of work that is not authorized under this Task Order. No payments will be made for any unauthorized supplies and/or services or for any unauthorized changes to the work specified herein. This includes any services performed by the Contractor on their own volition or at the request of an individual other than a duly appointed CO, COTR, or Government Technical Representative. Only a duly appointed CO is authorized to change the specifications, terms, or conditions under this effort.

17.13 Payment for Correction of Defects

The Contractor will not be paid for re-performance of defective or deficient fixed priced services [FAR 52-246-4(e) Inspection of Services-FP] or profit associated with re-performance of any defective or deficient time and material or labor hour work [FAR 52-246-6 (f) Inspection-T&M].

ATTACHMENTS

Attachments to the PWS include:

- Attachment A - FSD Contact Center Data
- Attachment B - FSD Issue Type Hierarchal Volume
- Attachment C - Notarized Letter Processing Data
- Attachment D - Contractor Employee Non-Disclosure Agreement
- Attachment E - Quality Assurance Surveillance Plan (QASP)